Les rapports du Conseil d'État

(ancienne collection
Étude et documents du Conseil d'État)

Fondateur

René Cassin

Comité de direction

Jean-Marc Sauvé, vice-président du Conseil d'État.

Bernard Stirn, Henri Toutée, Olivier Dutheillet de Lamothe, Bernard Pêcheur, Philippe Martin, Christian Vigouroux, Maryvonne de Saint Pulgent, présidents de section, François Séners, secrétaire général du Conseil d'État.

Jacky Richard, président adjoint et rapporteur général de la section du rapport et des études.

Directeur de la publication : Maryvonne de Saint Pulgent, présidente de la section du rapport et des études.

Secrétaire de rédaction : Corinne Mathey, secrétaire de la section du rapport et des études

Publications du Conseil d'État chez le même éditeur

Collection « Les rapports du Conseil d'État » (ancienne collection « Études et documents du Conseil d'État », EDCE)

- Un siècle de laïcité (EDCE n° 55), 2004.
- Responsabilité et socialisation du risque (EDCE n° 56), 2005.
- Sécurité juridique et complexité du droit (EDCE n° 57), 2006.
- L'administration française et l'Union européenne :
- Quelles influences ? Quelles stratégies ? (EDCE n° 58), 2007.
- Le contrat, mode d'action publique et de production de normes (EDCE n° 59), 2008.
- Droit au logement, droit du logement (ECDE n° 60), 2009.
- L'eau et son droit (ECDE n° 61), 2010.
- Consulter autrement, participer effectivement, (EDCE n° 62), 2011.
- Les agences : une nouvelle gestion publique ? - étude annuelle 2012, n° 63, 2012.
- Le droit souple - étude annuelle 2013, n° 64, 2013.

Collection « Les études du Conseil d'État »

- Redevances pour service rendu et redevances pour occupation du domaine public, 2002.
- Collectivités territoriales et obligations communautaires, 2004.
- L'avenir des juridictions spécialisées dans le domaine social, 2004.
- Le cadre juridique de l'action extérieure des collectivités locales, 2006.
- Inventaire méthodique et codification du droit de la communication, 2006.
- Pour une politique juridique des activités spatiales, 2006.
- Pour une meilleure insertion des normes communautaires dans le droit national, 2007.
- Le droit de préemption, 2008.
- L'implantation des organisations internationales sur le territoire français, 2008.
- Les recours administratifs préalables obligatoires, 2009.
- La révision des lois bioéthiques, 2009.
- Les établissements publics, 2010.
- Développer la médiation dans le cadre de l'Union européenne, 2011.
- Vers l'institution d'un parquet européen, 2011.
- Le rescrit : sécuriser les initiatives et les projets, 2014.
- L'application du nouveau principe « silence de l'administration vaut acceptation », 2014

Collection « Droits et Débats »

- Le droit européen des droits de l'homme, 2011.
- Les développements de la médiation, 2012.
- La valorisation économique des propriétés des personnes publiques, 2012.
- La démocratie environnementale, 2012.
- Consulter autrement, participer effectivement, 2012.
- Santé et justice : quelles responsabilités ?, 2013.
- Le patrimoine immatériel des personnes publiques, 2013.
- Les agences : une nouvelle gestion publique ?, 2013.
- Les enjeux juridiques de l'environnement, n° 9, 2014.
- La décentralisation des politiques sociales, n° 10, 2014.
- 1952-2012 : le juge français de l'asile, n° 11, 2013.
- Corriger, équilibrer, orienter : une vision renouvelée de la régulation économique, Hommage à Marie-Dominique Hagelsteen, n° 12, 2014.

Le numérique et les droits fondamentaux

- **AVANT-PROPOS** 5
- **SYNTHESE** 9
- **INTRODUCTION** 35
- Première partie – **L'ESSOR DU NUMÉRIQUE A SUSCITÉ LA RECONNAISSANCE DE NOUVEAUX DROITS FONDAMENTAUX ET MODIFIÉ LEURS CONDITIONS D'EXERCICE** 41
- Deuxième partie – **L'AMBIVALENCE DU NUMÉRIQUE NÉCESSITE DE REPENSER LA PROTECTION DES DROITS FONDAMENTAUX** 153
- Troisième partie – **METTRE LE NUMÉRIQUE AU SERVICE DES DROITS INDIVIDUELS ET DE L'INTÉRÊT GÉNÉRAL** 261
- **CONCLUSION** 333
- **RÉCAPITULATIF DES MESURES PROPOSÉES** 337
- **ANNEXES** 351
- **CONTRIBUTIONS** 391
- **LISTE DES ABRÉVIATIONS ET DES ACRONYMES** 435
- **TABLE DES MATIÈRES** 439

L'étude annuelle 2014 du Conseil d'État a été rédigée par Jacky Richard, conseiller d'État, rapporteur général de la section du rapport et des études et par Laurent Cytermann, maître des requêtes, rapporteur général adjoint. Tristan Aureau et Angélique Delorme, auditeurs au Conseil d'État, ont apporté leur concours.

Dans le cadre de leur stage à la section du rapport et des études, Ariane Bakkali, Jean-Philippe Besson, Hortense Chalvin, Edouard Jousselin, Julia Masini, Nicolas Pesme et Mathilde Teissier ont participé aux travaux, notamment en contribuant aux recherches documentaires. Anne Fontanille, avocate, en formation en master « management et protection des données à caractère personnel » et stagiaire à la section du rapport et des études, a assuré une contribution particulière à l'étude dans le domaine du droit européen et du droit de la concurrence. Qu'ils en soient vivement remerciés

Avant-propos

Par Jean-Marc Sauvé,
vice-président du Conseil d'État

Alors qu'une révolution technologique, comparable dans ses effets à celle qui suivit l'invention de l'imprimerie à l'époque moderne, continue de bouleverser les processus économiques de production et de consommation à l'échelle mondiale, les conséquences juridiques de ce phénomène apparaissent désormais avec plus de netteté. Les technologies de l'internet et les espaces numériques qu'elles ont engendrés n'invitent pas seulement les juristes à l'exploration et à la conquête d'une nouvelle *terra incognita* ; ils transforment de l'intérieur, voire dérèglent, les conditions d'exercice des droits fondamentaux et les mécanismes traditionnels de leur conciliation. En consacrant son étude annuelle *(au) Numérique et (aux) droits fondamentaux*, le Conseil d'État met son expertise de conseiller des pouvoirs publics et de juge suprême de l'ordre administratif au service d'une réflexion sur la cohérence, la complétude, la pertinence et l'effectivité de notre ordonnancement juridique face aux mutations, toujours plus profondes, de nos modes de vie. Une nouvelle fois, il s'attache à penser des évolutions profondes de la société et leur impact sur les droits fondamentaux des individus et les intérêts généraux que les autorités publiques doivent assumer. Il est aussi conduit, par conséquent, à repenser le rôle de la puissance publique, dans ses modes d'intervention comme dans son cadre territorial : il se situe ainsi résolument dans l'État, mais aussi « *au-delà de l'État* »[1] .

Dans la lignée de ses précédentes études, le Conseil d'État a fait usage d'une méthode interdisciplinaire, empruntant leur cadre d'analyse aux économistes, aux ingénieurs, aux sociologues et naturellement aux juristes, et il a adopté une démarche ouverte et prospective, en auditionnant des élus, des entrepreneurs, des chercheurs, des responsables d'autorités indépendantes ainsi que les représentants d'institutions et d'associations. Conjurant le risque d'une vision platement kaléidoscopique, ces mises en perspective ont permis d'établir une cartographie des enjeux techniques, socio-économiques et géopolitiques du numérique. À l'aune de ces enjeux et dans un espace en recomposition et encore mouvant – comme l'illustrent les deux arrêts de la Cour de justice de l'Union européenne, *Digital Rights Ireland Ltd* et *Google Spain SL*, respectivement du 8 avril et du 13 mai 2014 –, ont été identifiées les imperfections et les lacunes du cadre juridique existant, mais aussi ce qui, en lui, demeure pertinent et opérationnel.

1. S. Cassese, *Au-delà de l'État*, Bruylant, avril 2011, préface de P. Cossalter.

Partant, a été mise en exergue l'ambivalence d'une technologie qui, tout à la fois, catalyse l'exercice des libertés fondamentales et synthétise des droits nouveaux, mais génère aussi des menaces redoutables et inédites à l'encontre des personnes et des intérêts dont les autorités publiques ont la charge. Sous l'effet de ces forces déstabilisatrices, les antinomies traditionnelles du droit public se sont intensifiées, une conciliation plus exigeante devant être opérée entre liberté d'expression et sauvegarde de l'ordre public, liberté d'information et protection de la vie privée, sûreté et lutte contre la criminalité, liberté d'entreprendre et respect des règles de concurrence. Le droit public lui-même est apparu comme l'un des termes d'une conciliation plus vaste, afin que l'édiction de normes nouvelles n'entrave pas, par des contraintes excessives et inhibantes, le développement économique de notre pays et, au-delà, du continent européen où résident près de 400 millions d'internautes.

Pour résoudre ces difficultés et anticiper leurs développements à venir, doit être engagé un double effort de lucidité et d'inventivité, auquel le Conseil d'État apporte, par cette étude, sa contribution. Il propose de mettre le numérique davantage au service des droits individuels comme de l'intérêt général. L'intervention publique doit accroître la capacité des personnes à agir pour la défense de leurs droits : les pouvoirs publics doivent savoir « s'allier avec la multitude ». Sont ainsi proposés de nouveaux principes régulateurs de l'accès aux réseaux et de l'usage des ressources numériques, comme celui de neutralité de l'internet et celui de loyauté dans la conservation, le référencement et la diffusion d'informations, en particulier lorsqu'elles sont personnelles et nominatives. La responsabilité de chaque acteur, celle des éditeurs et des hébergeurs mais aussi celle des plateformes, doivent à l'aune de ces principes être précisées. Parallèlement, il convient de définir un nouvel équilibre dans l'utilisation du numérique par les personnes publiques à des fins de répression de la criminalité ou de prévention des atteintes à la sécurité nationale. En outre, un travail de systématisation des différentes sources du droit applicable au numérique doit être poursuivi et l'élaboration d'un *corpus* de règles opérationnelles doit mobiliser tous les ressorts de la normativité, combinant des conventions internationales et des règles européennes ou nationales et utilisant, en complément des normes impératives, des instruments de droit souple.

La saisie croissante du numérique par le droit est à la fois une réalité et une nécessité. Elle doit être portée à un niveau supranational, d'abord à l'échelle européenne par la définition d'un socle commun de règles impératives, ensuite au niveau transatlantique en vue d'une gouvernance plus équilibrée et plus efficace des flux numériques. Les difficultés politiques, juridiques et techniques que soulève un tel objectif sont évidentes : elles ne sauraient entraver la recherche du plus grand consensus parmi les États dont les capacités de réglementation et de régulation sont réelles et doivent être coordonnées dans le cadre de nouvelles coopérations. Des choix stratégiques devront être opérés et une sécurisation juridique des usages du numérique, notamment en matière de données personnelles, est encore à assurer. La présente étude prend ainsi position dans les débats actuels en affirmant nettement que ces données ne doivent pas faire l'objet d'une appropriation patrimoniale mais que, pour autant, les intéressés

doivent disposer d'un droit de regard et conserver la maîtrise sur les données qui les concernent : c'est ce qu'elle nomme, après la Cour constitutionnelle fédérale d'Allemagne, « l'autodétermination informationnelle ».

Les perspectives que trace la présente étude sur les espaces déterritorialisés d'internet font ainsi apparaître à la communauté juridique et aux pouvoirs publics une nouvelle aire, parfois inhospitalière aux figures du régulateur et du juge, mais elles ébauchent aussi les linéaments d'un ordre juridique modernisé, à la texture plus ouverte et moins pyramidale, et lui-même devenu réseau des normes. Cet ordre juridique global, issu des États et des sociétés européennes, a vocation à se constituer en système juridique autonome et à s'imposer progressivement aux ordres juridiques nationaux. Tel est l'horizon de cette étude.

Le numérique et les droits fondamentaux

Le numérique, parce qu'il conduit à la mise en données et à la mise en réseau générale du monde, pose problème au regard des droits fondamentaux ; non qu'il serait un phénomène négatif en soi, mais parce qu'il met en question leur contenu et leur régime. En effet, il renforce la capacité des individus à jouir de certains droits, comme la liberté d'expression ou la liberté d'entreprendre ; il en fragilise d'autres comme le droit à la vie privée, la sûreté et le droit à la sécurité.

L'étude annuelle du Conseil d'État intervient alors que le phénomène prend une nouvelle dimension : un triple basculement se manifeste, dans les innovations techniques, dans l'économie et dans l'appréhension du numérique par la société, et renforce les interrogations sur les droits fondamentaux.

Après avoir exposé comment l'essor du numérique a déjà suscité la reconnaissance de nouveaux droits et libertés fondamentaux et modifié leurs conditions d'exercice (1re partie), l'étude montre pourquoi l'ambivalence du numérique impose de repenser la protection de ces droits (2e partie). Elle fait en ce sens cinquante propositions pour mettre le numérique au service des droits individuels comme de l'intérêt général (3e partie).

1. – L'essor du numérique a suscité la reconnaissance de nouveaux droits fondamentaux et modifié leurs conditions d'exercice

1.1. L'essor du numérique entraîne des mutations techniques, économiques et sociales

Le numérique se définit comme la représentation de l'information ou de grandeurs physiques (images, sons) par un nombre fini de valeurs discrètes, le plus souvent représentées de manière binaire par une suite de 0 et de 1. Sa puissance transformatrice tient à sa capacité à exprimer des réalités disparates (sons, images, textes, comportements humains, processus industriels ...) dans un langage commun universel ouvrant la possibilité de les traiter de manière systématique et de les mettre en relation. Il en résulte des mutations techniques, économiques et sociales.

Les mutations techniques découlent de la mise en réseau des machines et de la mise en données du monde. La mise en réseau des machines a été rendue possible par les choix d'architecture qui ont présidé à la conception d'internet dans les années 1960 et 1970 : l'ouverture qui permet à tout réseau local d'être connecté à l'internet sans contrôle d'une autorité centrale ; la neutralité, les routeurs utilisés dans les nœuds d'interconnexion étant indifférents au contenu du message. Ces choix ont permis l'expansion mondiale d'internet, qui compte aujourd'hui près de 3 milliards d'utilisateurs. La mise en données du monde est permise par la croissance du nombre d'utilisateurs, la puissance de calcul des machines et la présence de plus en plus diffuse de capteurs connectés.

Définie strictement, l'économie numérique se compose de quelques secteurs spécialisés tels que les télécommunications, l'édition de logiciels ou les sociétés de services et d'ingénierie informatique (SS2I) ; mais elle se déploie aujourd'hui bien au-delà et tend à transformer la quasi-totalité des secteurs d'activité : industries culturelles, presse, commerce et distribution, hôtellerie, transport de personnes, services financiers, automobile, bâtiment... Dans tous ces secteurs, le numérique manifeste sa capacité à bouleverser les règles du jeu et les positions établies. Les modèles d'affaires des entreprises du numérique présentent des caractéristiques spécifiques : une orientation vers la croissance plutôt que la profitabilité à court terme, des stratégies de redéfinition des frontières des marchés dans lesquels elles opèrent, des stratégies de plateforme qui leur confèrent une position de porte d'accès aux consommateurs et enfin une valorisation intensive des données, notamment des données personnelles.

Les effets du numérique transforment aussi les relations sociales. Le numérique agit comme un multiplicateur de collaborations, qui se manifestent sous diverses formes : développement des services de partage, plateformes d'échanges de contenus, réseaux sociaux... Il favorise la participation et la transparence dans l'action des pouvoirs publics. Son impact sur les normes sociales fait débat, notamment en matière de vie privée. Aux tenants d'un dépassement de l'aspiration à la vie privée, en faveur d'un mouvement de « *publicisation de soi* », s'opposent ceux qui soutiennent que cette aspiration n'a pas disparu mais a seulement changé de contenu : il ne s'agit plus seulement d'être « laissé en paix », à l'abri des intrusions, mais aussi de maîtriser son image de soi et sa réputation.

1.2. Le numérique a suscité la reconnaissance de nouveaux droits fondamentaux : le droit à la protection des données personnelles et le droit d'accès à internet

Le droit à la protection des données personnelles (a) et le droit d'accès à internet (b) sont nés en réponse aux questions posées par l'essor du numérique. S'ils sont souvent présentés comme se rattachant respectivement au droit à la vie privée et à la liberté d'expression, leurs enjeux sont en réalité plus larges et peuvent être considérés comme des droits fondamentaux autonomes.

(a) Dans sa courte histoire, le droit à la protection des données personnelles aura connu un bouleversement complet des enjeux qui y sont associés : les auteurs du Rapport Tricot de juin 1975, dont les préoccupations principales portaient sur les conséquences de la constitution de grandes bases de données administratives, ne pouvaient envisager ni l'essor d'internet, ni la puissance de calcul dont disposeraient des terminaux mobiles, ni la valeur économique acquise par les données. Le cadre légal issu de ces réflexions s'est pourtant avéré d'une grande stabilité, ne donnant lieu qu'à une seule réforme importante, intervenue pour transposer la directive n° 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995 et qui a notamment déplacé l'accent du secteur public vers le secteur privé.

Les différentes normes applicables en matière de protection des données personnelles (Constitution, convention n° 108 du Conseil de l'Europe du 28 janvier 1981, Charte des droits fondamentaux de l'Union européenne, directive n° 95/46/CE et loi du 6 janvier 1978 modifiée) convergent aujourd'hui quant aux principales garanties de la protection des données personnelles :

- principes relatifs à la qualité des données (loyauté de la collecte, finalités légitimes, proportionnalité, durée de conservation) ;

- exigence du consentement de la personne concernée ou d'un autre fondement légitime prévue par la loi ;

- interdiction de la collecte des données dites sensibles, sauf dans des cas particuliers prévus par la loi ;

- droits d'information, d'accès, de rectification et d'opposition;

- obligation de sécurité du responsable du traitement ;

- existence d'une autorité indépendante de contrôle.

Ces principes constituent le socle d'un droit européen des données personnelles, substantiellement différent du droit américain.

(b) La Cour suprême des États-Unis a été la première juridiction souveraine à être saisie des enjeux de l'accès à internet pour la liberté d'expression, dans un arrêt *Reno, Attorney general of the United States vs American Civil Liberties Union (ACLU)* du 26 juin 1997. En France, le Conseil constitutionnel s'est prononcé à l'occasion d'un recours contre la loi favorisant la diffusion et la protection de la création sur internet : il a jugé à cette occasion que la liberté de communication protégée par l'article 11 de la Déclaration des droits de l'homme et du citoyen « *implique la liberté d'accéder à ces services* » (décision n° 2009-580 DC du 10 juin 2009, §12).

La reconnaissance de l'accès à internet comme un droit fondamental oblige à garantir l'égalité de traitement des particuliers et des entreprises dans cet accès : c'est l'enjeu des débats sur la « neutralité du net », concept formulé pour la première fois en 2003 par le juriste américain Tim Wu. La neutralité du net implique que tous les opérateurs de communications traitent de manière

égale tous les flux de données quel que soit leur contenu. Elle correspond à l'architecture originelle d'internet, qui repose sur le principe du « meilleur effort » (« *best effort* ») : chaque opérateur fait de son mieux pour assurer la transmission de tous les paquets de données qui transitent par son réseau, sans garantie de résultat et sans discrimination. Plusieurs facteurs techniques, économiques et politiques conduisent cependant les opérateurs à différencier le traitement des paquets selon leur contenu. Les débats sur la neutralité du net ont pour objet de déterminer si ce principe doit être inscrit dans le droit positif afin de restreindre ces possibilités de différenciation. Ils revêtent un caractère à la fois technique, économique et politique.

1.3. Le numérique a entraîné de profondes modifications du régime juridique de plusieurs libertés fondamentales

L'essor du numérique favorise à l'évidence l'exercice de certains droits, tout en remettant en question certains aspects de leur régime juridique : c'est le cas de la liberté d'expression (a) et de la liberté d'entreprendre (b). Pour d'autres droits, comme le droit à la sécurité (c) et le droit de propriété intellectuelle (d), le numérique se présente davantage comme un risque, auquel le législateur doit parer.

(a) Si la **liberté d'expression** est le principe fondamental commun à tous les moyens de communication, le régime juridique qui en définit les conditions d'exercice n'est pas le même selon le *medium* employé. Jusqu'à l'émergence d'internet, il y avait une parfaite superposition entre la forme d'expression (presse, communication téléphonique et communication audiovisuelle), le moyen technique employé et le régime juridique. Internet met en question ces distinctions, puisqu'il permet de diffuser par le même *medium* des contenus relevant de la correspondance privée, de la presse et de l'audiovisuel, phénomène souvent qualifié de « convergence ».

Le régime juridique de la liberté d'expression sur internet est relativement stable depuis la loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique (LCEN). En cohérence avec l'architecture d'internet, il encadre de manière distincte la couche des infrastructures et la couche des contenus. Dans ce dernier cas, la LCEN a défini deux grandes catégories d'acteurs : les éditeurs d'une part, soumis à un régime très voisin de celui de la presse, les hébergeurs d'autre par, dont le régime de responsabilité civile et pénale est atténué par rapport à celui des éditeurs, puisqu'ils sont regardés comme n'exerçant pas de contrôle sur les contenus accessibles par leur site.

Le régime de la communication sur internet, qu'il s'agisse de celui des éditeurs ou *a fortiori* de celui des hébergeurs, est ainsi marqué par un grand libéralisme qui le distingue du régime de la communication audiovisuelle, lequel institue une autorisation préalable assortie d'obligations diverses pour les fournisseurs de contenus. Le développement de la consommation audiovisuelle sur internet, notamment de films et de séries télévisées, conduit à de nouvelles interrogations

sur cet écart, qui peut constituer une distorsion de concurrence et fragiliser la politique française de soutien à la création et à la production de contenus culturels.

Internet soulève aussi de nouvelles questions quant aux limites de la liberté d'expression et à la lutte contre les contenus illicites. Les textes constitutionnels et conventionnels qui garantissent la liberté d'expression reconnaissent tous la possibilité de lui imposer certaines limites et, par lui-même, internet ne remet en cause ni l'existence de ces limites ni leur tracé. Toutefois, les spécificités d'internet conduisent à s'interroger sur l'efficacité des mesures prises par les pouvoirs publics à l'encontre des contenus illicites et sur le rôle reconnu aux acteurs privés dans la lutte contre ces contenus. Si l'intervention des intermédiaires de l'internet peut apparaître salutaire pour assurer une protection efficace d'intérêts publics tels que la lutte contre la xénophobie ou la protection des mineurs, elle suscite des débats sur sa légitimité.

(b) Les bouleversements économiques suscités par le numérique ont une incidence sur le droit des activités économiques. La **liberté d'entreprendre** implique désormais le droit à une existence numérique. La loi et la jurisprudence garantissent aujourd'hui ce que l'on pourrait qualifier de « droit à une existence numérique » de l'entreprise, qui comporte plusieurs éléments : droit à un nom de domaine, droit à fournir des services sur internet, droit d'utiliser certains instruments tels que la publicité, la cryptographie ou les contrats conclus par voie électronique.

Les mutations associées au numérique compliquent la mise en œuvre des deux formes d'encadrement de la liberté d'entreprendre, la régulation générale de la concurrence et les réglementations sectorielles applicables à certaines activités. On observe d'abord dans de nombreux secteurs de l'économie numérique une progressive concentration du marché autour d'un ou plusieurs acteurs prééminents, qui est favorisée par les rendements d'échelle croissants, les effets de réseau et le rôle central des plateformes. Ces acteurs dominants sont conduits à étendre constamment leur activité à de nouveaux services et à racheter les opérateurs émergents susceptibles de leur faire concurrence.

L'économie numérique bouscule aussi de nombreuses réglementations sectorielles car elle confronte les acteurs établis avec de nouveaux intervenants qui contestent l'applicabilité de la règle sectorielle ou dont le modèle d'affaires repose sur une logique différente. C'est notamment le cas dans le domaine des télécommunications, du livre, de l'hôtellerie, des taxis et de l'assistance aux justiciables.

(c) Le numérique permet ou favorise de nouveaux types d'atteintes à la sûreté et la sécurité, qui nécessitent des réponses juridiques. Il donne aussi à la police de nouveaux moyens qui appellent de nouvelles garanties pour préserver l'**équilibre entre sauvegarde de l'ordre public et liberté personnelle**.

Le numérique peut être la cible d'atteintes à la sécurité, ayant pour but d'accéder à des données confidentielles, de détruire ou d'altérer des données, d'entraver

le bon fonctionnement du système ou d'utiliser des ressources informatiques à l'insu de leur détenteur. La loi n° 88-19 du 5 janvier 1988 relative à la fraude informatique, dite « loi Godfrain », punit les faits d'accès frauduleux à un « *système de traitement automatisé de données* », d'entrave à leur fonctionnement ou encore de modification ou de suppression frauduleuse de données. L'État et les « opérateurs d'importance vitale » (OIV) n'échappent pas à la dépendance croissante de leur fonctionnement aux systèmes d'information. Pour faire face à ces attaques, ils ont complété les dispositifs existants de répression pénale en adaptant leurs moyens matériels (création en 2009 d'une agence spécialisée, l'Agence nationale de la sécurité des systèmes d'information (ANSSI)) et juridiques (pouvoir donné au Premier ministre par une loi de fixer des règles de sécurité des systèmes d'information qui s'imposent aux OIV). Le numérique peut aussi être utilisé pour porter atteinte à la sécurité : s'il n'est pas à l'origine de types de délinquance tels que la contrefaçon, l'escroquerie ou la pédophilie, il les facilite et en fait apparaître de nouvelles formes.

En sens inverse, le numérique renforce l'efficacité tant de la police judiciaire que de la police administrative et du renseignement. Il renforce l'efficacité de leurs modes opératoires préexistants, tels que les fichiers, l'usage de données biométriques ou la vidéosurveillance. Il rend également possibles de nouveaux modes d'investigation, notamment par la surveillance des communications électroniques et le recours aux nouveaux modes d'exploitation des données associés au *Big Data*.

Des garanties ont été instaurées par le législateur afin d'encadrer ces moyens nouveaux des services de police et de renseignement, notamment pour :

- la mise en œuvre des fichiers de sécurité, qui font l'objet d'un encadrement spécifique par la loi du 6 janvier 1978 modifiée ;

- la vidéosurveillance, soumise à un régime d'autorisation par la loi du 21 janvier 1995 ;

- l'interception des communications, la loi du 10 juillet 1991 ayant distingué les interceptions judiciaires des interceptions administratives de sécurité, et la loi du 23 janvier 2006 ayant complété ces régimes d'interception du contenu des communications par un régime de conservation et d'accès aux « métadonnées » (données sur les personnes participant à une communication, la durée de leur échange et leur localisation, également appelées données de connexion).

(d) Le **droit de la propriété intellectuelle** a été étendu à des objets issus des technologies numériques, les logiciels et les bases de données ; il joue ainsi dans l'économie numérique un rôle structurant. Prérogatives classiques du droit d'auteur, le droit de reproduction et le droit de représentation ont montré leur plasticité en s'appliquant à la numérisation et à la diffusion sur internet.

Pour autant, internet fait largement abstraction du droit de propriété intellectuelle en facilitant de manière considérable la reproduction et la diffusion des œuvres en méconnaissance du droit d'auteur et des droits voisins.

Les pouvoirs publics ont réagi en combinant prévention (recours et protection juridique des « mesures techniques de protection » entravant la copie, notification des contenus illicites aux hébergeurs), répression (mise en place par les lois du 12 juin 2009 et du 28 octobre 2009 d'un dispositif de « réponse graduée ») et promotion des usages licites.

1.4. Internet n'échappe ni en fait, ni en droit à la puissance étatique, mais lui pose des défis inédits

Contrairement à ce qu'avaient espéré ses pionniers, internet n'est pas un espace hors du droit. Les deux postulats de cette approche libertaire, le défaut de légitimité des États à réglementer internet et leur incapacité à le faire, n'ont pas été vérifiés. **Les États ne sont pas moins légitimes à légiférer sur les réseaux numériques** que sur tout autre domaine d'activité humaine. La capacité des États à exercer leur pouvoir sur internet est désormais avérée. L'illustration la plus extrême en est donnée par les pratiques d'États non démocratiques, qui parviennent à entraver de manière significative l'accès de leurs ressortissants à internet. Les États de droit exercent également, dans des cadres définis par la loi et sous le contrôle du juge, un pouvoir de contrainte sur internet, par exemple lorsque des tribunaux ordonnent le retrait d'un nom de domaine ou le déréférencement d'un site.

Que la puissance de l'État parvienne à s'exercer sur internet ne signifie pas qu'elle n'y rencontre pas **des difficultés particulières**. Celles-ci tiennent notamment au mode de **gouvernance d'internet**, à la détermination de **la loi applicable** et à **l'effectivité** des interventions de l'État.

Alors que les précédentes innovations technologiques (télécommunications, aviation...) avaient suscité la création d'organisations intergouvernementales spécialisées, la gouvernance d'internet se distingue par l'absence d'autorité centrale et le rôle joué par plusieurs instances de droit privé, agissant notamment par la voie du droit souple et dans lesquelles la place des États-Unis est prépondérante : ICANN pour la gestion des noms de domaine, IETF et W3C pour la définition des standards techniques, *Internet Society* et Forum pour la gouvernance d'internet et pour le traitement des questions politiques, économiques et de société liées à internet. Dans ce modèle qualifié de « **multiacteurs** », les États ne sont que des parties prenantes parmi d'autres.

En rendant accessibles aux internautes de chaque pays les contenus et les services proposés dans le monde entier, internet crée de très nombreux conflits entre les systèmes juridiques des différents États et les confronte ainsi à une double difficulté : d'une part, la complexité des règles de droit international privé, qui déterminent la loi applicable et la juridiction compétente, est source d'incertitudes ; d'autre part, ces règles peuvent désigner des juridictions et des lois étrangères. L'État est ainsi confronté à la possibilité que ses lois sur la protection des données personnelles, la liberté d'expression ou la propriété intellectuelle ne soient en définitive pas applicables à toutes les situations qu'il entend régir.

Internet pose enfin trois problèmes spécifiques pouvant amoindrir l'effectivité des interventions de l'État : la facilité de recréation d'un site internet ayant été convaincu d'activité illicite ; la nécessité d'obtenir l'exécution de décisions administratives ou juridictionnelles par des États étrangers ; le décalage entre la vitesse d'évolution de l'univers numérique et le temps des processus institutionnels et juridictionnels.

* *

De ces multiples évolutions du droit du numérique se dégagent deux tendances qui déterminent la manière dont la protection des droits fondamentaux doit aujourd'hui être repensée : le numérique ouvre de nouveaux espaces aux libertés, notamment en matière d'expression, d'association, de sociabilité ; il est aussi un enjeu stratégique suscitant une vive compétition entre États et entre acteurs économiques.

2. – L'ambivalence du numérique nécessite de repenser la protection des droits fondamentaux

Face à l'explosion numérique, le droit s'est déjà beaucoup transformé. Il n'est pourtant pas parvenu à un point d'équilibre. Les interrogations sur la pertinence du régime juridique des droits fondamentaux se succèdent au même rythme que celui des innovations dont le numérique est porteur. La difficulté d'y répondre tient à **l'ambivalence intrinsèque** du phénomène numérique : il ouvre de nouveaux espaces de libertés, tout en étant porteur de risques pour celles-ci. Une intervention trop rigoureuse du législateur destinée à **prévenir les aspects négatifs** du numérique **risque**, du même mouvement, **d'en entraver le potentiel positif**. Pour surmonter cette difficulté, il faut repenser les modes de protection des droits fondamentaux pour les adapter à l'explosion des données, au rôle inédit des grandes « plateformes » et au caractère transnational d'internet.

2.1. L'explosion des usages des données personnelles et des risques associés conduit à en repenser la protection

• *Les risques liés à l'explosion des données personnelles*

Depuis l'adoption de la loi du 6 janvier 1978, les sources et les types de données personnelles en circulation se sont considérablement diversifiées. Les données ne sont plus seulement collectées par des entités organisées (administrations, entreprises, associations), mais aussi mises en ligne par les individus eux-mêmes ou par des tiers ou recueillies de manière automatique. Elles ne correspondent plus seulement aux caractéristiques objectives de l'individu (âge, sexe, profession...) ; il peut s'agir d'informations sur ses goûts, ses opinions, ses relations, ses déplacements ou encore de signaux biologiques ou corporels.

Si toutes ces informations restaient disséminées auprès des personnes qui les ont recueillies, les risques pour la vie privée seraient sans doute limités. La dynamique de l'économie numérique pousse cependant à leur regroupement. Le numérique a suscité l'émergence d'acteurs nouveaux, tels les moteurs de recherche ou les réseaux sociaux, qui sont dépositaires, par leur fonction, de pans entiers de notre vie personnelle. La publicité joue en la matière un rôle particulier : plus le nombre d'informations détenues sur **le « profil »** d'une personne est grand, plus les publicités qui lui sont adressées seront potentiellement pertinentes. Les grandes entreprises du numérique sont engagées dans des stratégies de diversification dont l'un des objectifs est de multiplier les données détenues sur chaque individu. Il existe aussi des acteurs spécialisés dans la collecte et la revente des données, les ***data brokers*** ; le plus important d'entre eux affirme détenir des données sur 700 millions de personnes dans l'ensemble du monde.

Cette diffusion généralisée des données personnelles et la tendance des acteurs économiques à les regrouper sont porteuses de **risques** pour les individus, que l'étude classe en **six catégories** : la diffusion de données personnelles en dehors de la volonté de l'individu concerné ; la réception de plus en plus fréquente de publicités de plus en plus ciblées et personnalisées ; le développement de pratiques commerciales abusives, consistant en une différenciation entre les clients à partir de l'exploitation de leurs données ; les risques de réputation, pouvant conduire à des restrictions dans l'accès à l'assurance, au crédit, à l'emploi ; les utilisations malveillantes, portant directement atteinte aux biens ou aux personnes ; l'utilisation des données personnelles par les pouvoirs publics à des fins de sauvegarde de l'ordre public et de la sécurité nationale, lorsqu'elle est excessive.

• *Un cadre juridique dont les principes fondamentaux demeurent pertinents, mais dont les instruments doivent être profondément transformés*

Les nouveaux risques liés au numérique suscitent des interrogations sur la pertinence du cadre juridique actuel de la protection des données personnelles. **Les principes fondamentaux de la protection des données résistent cependant à ces interrogations** :

- **Une définition large des données à caractère personnel** (couvrant notamment l'adresse IP et les « profils » utilisés en matière de publicité en ligne), telle que la préconise le G29, est nécessaire pour assurer la protection des personnes et c'est bien celle que retient la jurisprudence française.

- **Le principe de finalités déterminées** est au cœur de la confiance que les personnes peuvent avoir dans les services de la société numérique. C'est grâce à ce principe que les données personnelles ne sont pas des marchandises comme les autres : elles peuvent être échangées, mais le droit de propriété de leur acquéreur reste limité par les droits de la personne sur ses données, qui impliquent que leur utilisation soit limitée aux finalités pour lesquelles elles ont été initialement collectées.

- **Les principes de proportionnalité et de limitation de la durée** de conservation découlent de ce premier principe.

- Quant aux principes de loyauté de la collecte et d'exactitude des données traitées, ils ne sont que l'expression des principes généraux de la responsabilité.

- **Le rôle du consentement** de la personne ne doit être ni surestimé (dans la législation actuelle, il n'est ni une condition nécessaire ni une condition suffisante de la licéité du traitement des données), ni méconnu, car il incarne la liberté de la personne en matière d'utilisation de ses données personnelles.

Ces principes ne sont **pas une entrave au développement du *Big Data***. En effet, nombre des usages du *Big Data* ne visent pas les personnes en tant que telles, mais **l'exploitation statistique** des données les concernant. Or le principe de finalités déterminées n'exclut pas la liberté de réutilisation statistique : dans le cadre juridique actuel, la finalité statistique est toujours présumée compatible avec la finalité initiale du traitement. Lorsque les usages du *Big Data* visent les personnes en tant que telles, par exemple pour établir un profil prédictif de leurs caractéristiques (solvabilité, dangerosité...), la pleine application des principes fondamentaux de la protection des données est en revanche requise.

Si les principes conservent leur pertinence, **les instruments de la protection des données doivent être adaptés et renouvelés**. Quatre voies complémentaires devraient être explorées : l'utilisation des technologies pour renforcer la capacité des personnes à contrôler l'utilisation de leurs données ; la définition d'une « chaîne de responsabilités », allant des concepteurs de logiciels et d'objets connectés aux utilisateurs finaux et complétant la responsabilité du responsable de traitement ; une attention particulière portée à la circulation des données personnelles ; le passage d'une logique formelle de déclaration à une logique de respect en continu de la réglementation, assuré par des contrôles internes et externes.

Les évolutions en cours du droit de l'Union européenne s'engagent à juste titre dans la voie de la réaffirmation des principes et de la rénovation des instruments. En premier lieu, l'arrêt *Google Spain c/ AEPD* de la Cour de justice de l'Union européenne, en date du 13 mai 2014, **qualifie les moteurs de recherche de responsables de traitement des données personnelles** qu'ils collectent lorsqu'ils sont saisis de requêtes concernant un individu. Il en déduit l'existence d'**un droit au déréférencement**, fondé sur le droit d'opposition de la personne au traitement de ses données personnelles et sur le droit à l'effacement des données dont le traitement n'est pas conforme à la directive n° 95/46/CE. En se fondant sur les principes de la directive de 1995, la CJUE a donc créé un nouvel instrument adapté au problème de « l'e-réputation » de la société numérique contemporaine, dont la mise en œuvre devra toutefois veiller à une conciliation équilibrée avec la liberté d'expression (cf. *infra* **proposition n° 5**).

En second lieu, la Commission a adopté le 25 janvier 2012 **une proposition de règlement** relative aux données à caractère personnel, appelée à se substituer à la directive n° 95/46/CE. L'adoption de ce règlement par le Parlement européen

et le Conseil permettrait de mettre en place un corps de règles uniques dans l'ensemble de l'Union européenne et de **placer ainsi la protection à un échelon continental** plus adapté au caractère transnational d'internet. Le règlement rénove nombre d'instruments, notamment en supprimant l'obligation de déclaration des traitements qui revêtait un caractère trop formaliste, en rendant obligatoire la désignation de « délégués à la protection des données » par les responsables de traitement, en introduisant le concept de protection de la vie privée dès la conception (« *privacy by design* ») et en instaurant des sanctions administratives dissuasives. Si ces évolutions sont bienvenues, d'autres innovations peuvent être encouragées, notamment les technologies de renforcement de la vie privée ou le développement de la certification et de la corégulation.

• *La surveillance des communications par les pouvoirs publics présente des enjeux spécifiques et appelle des réponses adaptées*

Les principes de la surveillance des communications par les pouvoirs publics ont été fixés par la loi du 10 juillet 1991. Celle-ci a réaffirmé le secret des communications et n'a permis d'y porter atteinte que dans deux hypothèses, sur décision de l'autorité judiciaire ou, « à titre exceptionnel » et pour des finalités définies par la loi, sur décision du Premier ministre et sous le contrôle de la Commission nationale de contrôle des interceptions de sécurité (CNCIS). Depuis lors cependant, les pratiques de surveillance des communications par les pouvoirs publics et leur contexte ont profondément évolué, suscitant d'importants débats sur leur place et les garanties qui doivent les entourer. L'essor des communications électroniques et des capacités de stockage et d'analyse des données a démultiplié les possibilités d'interception. Les deux derniers livres blancs sur la défense ont fait de la collecte de renseignements par cette voie l'une des priorités de la politique de sécurité nationale de la France, qui s'est traduite par une forte augmentation des moyens matériels des services. Pus récemment, l'arrêt *Digital Rights Ireland* du 8 avril 2014 de la CJUE a remis en cause le cadre européen de la conservation des données et les révélations de ce qu'il est convenu d'appeler « l'affaire Prism » ont, partout dans le monde, porté ces sujets au premier plan du débat public. Alors que depuis la loi du 10 juillet 1991, le législateur a procédé en la matière par extensions successives du champ de la collecte de renseignement, il apparaît nécessaire aujourd'hui de procéder à un réexamen global du cadre juridique de la surveillance des communications, dans le but de **préserver la capacité de notre pays à protéger sa sécurité nationale tout en apportant l'ensemble des garanties nécessaires à la protection des droits fondamentaux, et notamment de la sûreté**.

Par son arrêt *Digital Rights Ireland*, la CJUE a déclaré invalide la directive n° 2006/24/CE du 15 mars 2006, qui prévoyait que les États devaient imposer aux opérateurs de communications de conserver pendant une durée comprise entre six mois et deux ans l'ensemble des données de connexion de leurs utilisateurs, en vue de garantir la disponibilité de ces données à des fins de recherche, de détection et de poursuite d'infractions graves. Elle a jugé que cette obligation générale de conservation constituait une ingérence particulièrement grave dans

les droits à la vie privée et à la protection des données personnelles garantis par les articles 7 et 8 de la Charte des droits fondamentaux de l'Union européenne ; si elle admet que cette ingérence est justifiée par des buts d'intérêt général tels que la lutte contre le terrorisme et la criminalité organisée, elle considère qu'elle n'est pas proportionnée, dès lors que la directive couvre les données de toute personne, ne prévoit aucune garantie concernant l'accès aux données conservées et fixe la durée de conservation sans tenir compte de l'utilité de la conservation par rapport aux objectifs poursuivis.

L'arrêt de la CJUE soulève la question de la conformité au droit de l'Union européenne des législations nationales, telles que la législation française, qui prévoient une telle obligation de conservation générale des données de connexion.

Compte tenu des enjeux de la surveillance des communications pour la protection de la sécurité nationale, l'étude du Conseil d'État ne propose pas de supprimer cette obligation mais préconise de renforcer les garanties concernant l'accès et l'utilisation de ces données.

2.2. Promouvoir les libertés à l'ère des « plateformes »

Le numérique favorise à l'évidence l'exercice de la liberté d'expression, de la liberté d'entreprendre et de la liberté d'association. Cependant il favorise aussi les comportements illicites, tels que les abus de la liberté d'expression et la contrefaçon. Par ailleurs, les situations d'inégalité de puissance et d'allocation de ressources rares peuvent justifier, comme dans d'autres domaines de la vie économique et sociale, l'intervention des pouvoirs publics pour promouvoir la plus grande liberté possible pour chacun.

• *Neutralité des réseaux, loyauté des plateformes et lutte contre les contenus illicites*

L'étude du Conseil d'État propose de **consacrer dans le droit positif** le principe de **neutralité du *net***, car il constitue une garantie fondamentale des libertés énumérées ci-dessus, en permettant à toute entreprise, toute association ou tout particulier de bénéficier d'un égal accès à tous les internautes. Les menaces qui pèsent aujourd'hui sur le respect de ce principe sont en outre plus consistantes qu'aux débuts d'internet, en raison de la position dominante de certains fournisseurs de contenus et de la part du trafic représentée par quelques grands sites de diffusion de vidéos. Il importe cependant, dans le cadre de la proposition de règlement de l'Union européenne (« quatrième paquet télécoms »), de prévoir une définition suffisamment large des « services spécialisés », dans le cadre desquels les opérateurs peuvent proposer un niveau de qualité garanti et supérieur à celui de l'internet généraliste. Le développement de ces services spécialisés est en effet nécessaire pour proposer des usages innovants tels que, par exemple, la télémédecine. En contrepartie de cette définition large, les autorités de régulation des communications électroniques devraient disposer de prérogatives suffisantes pour empêcher les services spécialisés de nuire à la qualité de l'internet généraliste.

Les opérateurs de communications électroniques ne sont pas les seuls acteurs à jouer un rôle déterminant dans l'exercice des libertés sur internet : la situation des « **plateformes** » doit également être traitée. Cette expression désigne usuellement les sites qui permettent à des tiers de proposer des contenus, des services ou des biens ou qui donnent accès à de tels contenus : magasins d'applications, sites de partage de contenus, places de marché, moteurs de recherche... Le rôle d'intermédiation confère aux plateformes un pouvoir, à la fois économique et de prescription, qui a une forte incidence sur l'exercice par les tiers de leurs libertés et pose aux pouvoirs publics des questions inédites.

L'étude du Conseil d'État relève d'abord que la *summa divisio* prévue par l'article 6 de la LCEN, qui transpose la directive « commerce électronique » de 2000, entre les intermédiaires techniques, dont la responsabilité civile et pénale est limitée, et les éditeurs de site, n'est plus adaptée face au rôle croissant des plateformes. En effet, nombre de plateformes ne se contentent pas de stocker passivement les offres des sociétés tierces ou les contenus mis en ligne, elles les organisent en les indexant et en faisant, le cas échéant, des recommandations personnalisées aux internautes. Plusieurs arrêts de la CJUE et de la Cour de cassation ont montré qu'une place de marché ou un moteur de recherche ne répondaient pas à la condition de rôle purement technique et passif prévue par la directive de 2000 pour bénéficier de la qualité d'hébergeur et du régime de responsabilité limitée qui lui est associé. La responsabilité limitée joue pourtant un rôle essentiel dans l'exercice des libertés sur internet, en évitant aux plateformes de procéder à une censure préventive des contenus mis en ligne pour ne pas voir leur responsabilité engagée. Il apparaît donc nécessaire de créer **une nouvelle catégorie juridique, celle des plateformes**, dont la définition ne reposerait plus sur le caractère technique et passif de leur rôle, mais sur le fait qu'**elles proposent des services de classement ou de référencement de contenus, biens ou services mis en ligne par des tiers**.

Les plateformes ne peuvent être soumises à la même obligation de neutralité que les opérateurs de communications électroniques, car leur rôle est de fournir un accès organisé, hiérarchisé ou personnalisé aux contenus mis à disposition sur leur site ou auxquels elles donnent accès : un traitement égalitaire ne peut être demandé à un moteur de recherche, puisque l'objet même d'un moteur de recherche est de hiérarchiser les sites internet. En revanche, **les plateformes devraient être soumises à une obligation de loyauté envers leurs utilisateurs**, tant les utilisateurs non professionnels **dans le cadre du droit de la consommation** que les utilisateurs professionnels dans le cadre **du droit de la concurrence**.

Parce qu'elles jouent un rôle de porte d'entrée pour la diffusion ou pour l'accès aux contenus sur internet, les plateformes sont impliquées dans les débats concernant la lutte contre les contenus illicites. Outre leurs obligations légales lorsqu'elles sont saisies de signalements de tels contenus, elles mettent aussi en place des **démarches volontaires dans le cadre de « politiques » relatives aux contenus** qu'elles acceptent ou d'outils de détection des contrefaçons qu'elles mettent à la disposition des ayants droit. Ce rôle est l'objet de controverses,

certains acteurs le qualifiant de « police privée ». Le Conseil d'État considère qu'il ne serait pas réaliste de dénier aux acteurs privés le droit de décider du retrait d'un contenu et de réserver ce droit au juge. En revanche, il importe de mieux garantir les droits des personnes faisant l'objet d'une mesure de retrait, qui ne disposent souvent pas de possibilités de faire valoir leurs observations. En outre, le pouvoir de fait considérable associé à la définition des « politiques » relatives aux contenus devrait s'exercer dans des conditions plus grandes de transparence et de concertation avec les parties prenantes.

• *La nécessité de doter la régulation audiovisuelle d'instruments adaptés à l'environnement numérique*

Deux des fondements théoriques de la régulation audiovisuelle, l'occupation du domaine public et la nécessité de réglementer des programmes « linéaires », ne peuvent être transposés aux services audiovisuels accessibles par internet. Le premier est tiré des règles générales de la domanialité publique qui permettent à la personne publique d'imposer des obligations d'intérêt général aux occupants et ne peuvent s'appliquer aux services audiovisuels diffusés par internet, lesquels ne passent pas par l'utilisation privative du domaine public hertzien. Le second fondement tient à ce qu'il est convenu d'appeler le caractère « linéaire » des services audiovisuels classiques. Sur internet, l'utilisateur peut passer comme il le souhaite d'un site à un autre et dispose donc d'une plus grande liberté de choix.

En revanche, un troisième fondement théorique est aussi pertinent sur internet que sur les moyens de communication audiovisuels classiques : celui des objectifs de valeur constitutionnelle que sont la sauvegarde de l'ordre public, le respect de la liberté d'autrui et la préservation du caractère pluraliste des courants d'expression socioculturels, ainsi que de l'intérêt général qui s'attache à la promotion de la diversité culturelle.

Afin de ne pas porter atteinte à la neutralité du net, l'étude propose de ne pas imposer aux opérateurs de communications de procéder à une différenciation entre des contenus licites dans le cadre de l'internet généraliste. En revanche, de telles obligations sont envisageables dans le cadre de la distribution de services spécialisés.

• *Prendre la mesure du rôle joué par les algorithmes et concevoir l'encadrement de leur utilisation*

L'algorithme est au cœur du rôle d'intermédiation joué par les plateformes. L'usage des algorithmes n'est cependant pas réservé aux plateformes et le développement du *Big Data* conduit à les appliquer dans de très nombreux domaines. L'utilité des algorithmes pour optimiser le fonctionnement d'un certain nombre de services n'est pas discutable. Ils présentent cependant trois sources de risques pour l'exercice des libertés : l'enfermement de l'internaute dans une « personnalisation » dont il n'est pas maître ; la confiance abusive dans les résultats d'algorithmes perçus comme objectifs et infaillibles ; de nouveaux problèmes d'équité du fait de l'exploitation toujours plus fine des données personnelles.

L'encadrement de l'utilisation des algorithmes est un domaine nouveau pour les pouvoirs publics, mais devenu nécessaire en raison du rôle grandissant de ces mécanismes et des risques qu'ils présentent pour l'exercice des libertés. L'étude du Conseil d'État préconise trois méthodes d'encadrement : assurer l'effectivité de l'intervention humaine dans la prise de décision au moyen d'algorithmes ; mettre en place des garanties de procédure et de transparence lorsque les algorithmes sont utilisés pour prendre des décisions à l'égard d'une personne ; développer le contrôle des résultats produits par les algorithmes, notamment pour détecter l'existence de discriminations Illicites.

2.3. Rendre applicable un socle de règles impératives pour tous les acteurs du numérique, quel que soit leur lieu d'établissement

La question du droit territorialement applicable sur internet constitue un enjeu de simplification et d'accessibilité du droit, mais également un enjeu stratégique, car elle met en cause la capacité des États à assurer la protection des libertés fondamentales de leurs citoyens ainsi que le droit au recours de ceux-ci. Les implications pour la concurrence entre entreprises numériques sont significatives.

• *Définir un socle de règles impératives applicables à tous les acteurs quel que soit leur lieu d'établissement*

La plupart des grandes entreprises du *net* étant établies aux États-Unis, la grande masse **des particuliers et des entreprises européennes se voient opposer la compétence juridictionnelle et la législation des différents États américains**, prévues par les conditions générales d'utilisation de ces services. Il serait cependant hâtif d'en déduire que les États européens ont intérêt à réclamer l'application systématique à leurs internautes de leurs règles de droit, quel que soit le pays d'origine du site internet. Il est en effet difficilement envisageable que le principe du pays de l'internaute devienne une règle générale et absolue de détermination de la loi applicable sur internet, car il ne peut être raisonnablement demandé à un site de se conformer à toutes les règles de droit de tous les pays du monde, ne serait-ce que parce qu'elles sont sur bien des points contradictoires entre elles, et que se conformer à certaines d'entre elles pourrait le mettre en infraction avec les règles de son propre État. Une telle orientation postulerait en outre que les acteurs français ou européens sont toujours voués à être sur internet en tant que consommateurs et non en tant que producteurs de services.

Le Conseil d'État préconise donc de **promouvoir le principe du pays de destination, non pour l'ensemble des règles juridiques applicables aux acteurs d'internet, mais pour un socle de règles** choisies en raison de leur importance particulière dans la protection des droits fondamentaux ou de l'ordre public. Les règles du socle seraient applicables à tous les sites dirigeant leur activité vers la France ou l'Union européenne (selon que la règle est de niveau national

ou européen), la notion d'activité dirigée vers un pays ayant le sens qui lui a été donné par la jurisprudence.

Selon les sujets, trois méthodes peuvent faire prévaloir le principe du pays de destination :

- l'application des règles de droit commun du droit international privé, qui permet notamment d'aboutir au résultat recherché en matière pénale ;

- **la qualification de « loi de police »** au sens du droit international privé, qui devrait être retenue **en matière de protection des données personnelles** et **d'obligations de coopération des acteurs privés** avec les autorités judiciaires et administratives agissant **à des fins de sécurité nationale** ;

- la coordination des législations nationales par un traité ou un acte de droit dérivé de l'Union européenne, qui pourrait être envisagée pour faire prévaloir le principe du pays de destination en matière d'audiovisuel.

• *Assurer une coopération efficace dans l'application, au sein de l'Union européenne et avec les autres systèmes juridiques*

Il revient aux États ou à l'Union européenne de fixer le champ d'application de leurs règles de droit. L'exécution de ces règles par des acteurs issus d'autres États implique en revanche une bonne coopération avec ces derniers. Trois types de relations sont abordés par l'étude : les relations entre États de l'Union européenne, dans la perspective de l'entrée en vigueur de la proposition de règlement relatif à la protection des données personnelles ; les relations entre l'Union européenne et les États-Unis ; les relations avec les autres systèmes juridiques.

Au sein de l'Union européenne, la désignation d'une **« autorité chef de file »** pour les responsables de traitement établis dans plusieurs États membres est nécessaire pour assurer l'efficacité de la régulation. Elle doit **cependant s'accompagner de mécanismes efficaces de coordination entre autorités** afin de prévenir les risques de « *forum shopping* » ainsi que de garanties du droit au recours des particuliers.

S'agissant des relations **avec les États-Unis**, le mécanisme du « ***Safe Harbour*** » devrait **être profondément réformé**. Sa renégociation avec le gouvernement américain doit porter sur deux questions : le passage d'une logique de déclaration d'engagements et d'autocertification à une logique de réglementation contraignante pour les entreprises adhérentes, assortie d'une intensification des contrôles par les autorités ; l'évolution du contenu des obligations contenues dans le *Safe Harbour*, les obligations actuelles étant souvent floues et éloignées du niveau de protection garanti en Europe.

S'agissant des relations **avec les autres systèmes juridiques**, la **convergence sur les valeurs** avec certains États, comme le Brésil et la Corée du sud, **permet d'envisager une politique plus ambitieuse** de reconnaissance mutuelle et d'actions conjointes de contrôle. La coopération en matière de lutte contre la

cybercriminalité devrait être intensifiée, par exemple par la mise en place d'un groupe d'action interétatique qui définirait des recommandations détaillées sur les pratiques de coopération à mettre en place et qui publierait des listes d'États non coopératifs.

3. – Mettre le numérique au service des droits individuels et de l'intérêt général

Aujourd'hui, les droits reconnus aux individus se limitent, pour l'essentiel, à leur permettre de rester à l'écart du traitement de leurs données (choix qui n'est presque jamais fait), sans leur donner de réel pouvoir sur le contenu du service et la manière dont leurs données sont traitées. Mettre le numérique au service des droits individuels, tel devrait être le premier principe directeur de la protection des droits fondamentaux dans les usages numériques. Par cette logique d'« *empowerment* », « d'autonomisation » des individus, l'intervention publique peut accroître la capacité des individus à agir pour la défense de leurs droits et à amplifier ainsi les possibilités d'action des pouvoirs publics eux-mêmes. Face à des acteurs du numérique dont le succès passe par leur relation privilégiée avec leurs utilisateurs, les pouvoirs publics doivent eux aussi savoir « s'allier avec la multitude ».

Le second principe directeur des propositions formulées dans cette troisième partie tend à mettre le numérique au service de l'intérêt général. Le numérique peut bénéficier de manière considérable à l'efficacité des politiques de santé, d'éducation, de culture, de sécurité ou de lutte contre la fraude, ainsi qu'à la simplification des démarches administratives ; encore faut-il que les personnes publiques disposent de cadres et d'instruments juridiques appropriés pour saisir ces opportunités, tout en assurant le respect des droits individuels. Il s'agit pour elles de concilier des droits fondamentaux entre eux ou des libertés avec des objectifs de valeur constitutionnelle : ainsi la sûreté à laquelle concourent la prévention et la répression des infractions les plus graves.

Même s'il reste un espace d'action autonome pour le droit interne, soit par la norme législative ou réglementaire, soit par le droit souple, nombre des propositions de cette étude relèvent de la compétence des institutions de l'Union européenne, soit parce qu'elles nécessitent une modification du droit de l'Union existant, soit parce que l'Union européenne constitue le niveau pertinent d'action.

3.1. Définir les principes fondant la protection des droits fondamentaux à l'ère du numérique

Il est parfois proposé de reconnaître aux individus un véritable droit de propriété sur leurs données, en pariant sur leur plus grande implication du fait qu'ils deviendraient financièrement intéressés à une bonne gestion de leurs données.

Le Conseil d'État ne recommande pas une telle orientation. S'il préconise de renforcer la dimension de l'individu acteur dans le droit à la protection des données, c'est en envisageant celui-ci comme un **droit à l'autodétermination** plutôt que comme un droit de propriété (**proposition n° 1**). La reconnaissance du droit de propriété ne permettrait pas en effet de rééquilibrer la relation entre les individus et les acteurs économiques et compliquerait l'exercice de la régulation par les pouvoirs publics. Le droit à « l'autodétermination informationnelle », concept dégagé par la Cour constitutionnelle allemande en 1983, est à la différence du droit de propriété un droit attaché à la personne, tendant à « garantir en principe la capacité de l'individu à décider de la communication et de l'utilisation de ses données à caractère personnel ». Ce droit ne devrait pas être défini comme un droit supplémentaire s'ajoutant aux autres droits (droit d'information, droit d'accès...), mais comme un principe donnant sens à tous ces droits, ceux-ci tendant à le garantir et devant être interprétés et mis en œuvre à la lumière de cette finalité.

Le principe de **neutralité des opérateurs de communications** électroniques doit être inscrit dans le droit positif, en prévoyant une définition large des services spécialisés assortie de pouvoirs importants des autorités de régulation pour veiller au maintien de la qualité générale d'internet (**proposition n° 2**). Les plateformes, qui constitueraient une nouvelle catégorie juridique, seraient quant à elles soumises à une obligation de loyauté, consistant à assurer de bonne foi le service de classement ou de référencement, sans chercher à l'altérer ou à le détourner à des fins étrangères à l'intérêt des utilisateurs (**proposition n° 3**).

3.2. Renforcer les pouvoirs des individus et de leurs groupements

Le renforcement des capacités d'action des individus doit intervenir à deux niveaux, individuel et collectif.

Au niveau individuel, l'étude du Conseil d'État préconise :

- de donner à la **CNIL** et à l'ensemble des autorités de protection des données européennes une mission explicite de **promotion des technologies** renforçant la **maîtrise des personnes** sur l'utilisation de leurs données (**proposition n° 4**) ;

- de mettre en œuvre de manière efficace le **droit au déréférencement** reconnu par la CJUE dans son arrêt *Google Spain,* notamment en donnant aux éditeurs des sites dont le déréférencement est demandé la possibilité de faire valoir leurs observations et en explicitant par des lignes directrices des autorités de protection des données leur doctrine de mise en œuvre de l'arrêt (**proposition n° 5**) ;

- de **définir les obligations des plateformes envers leurs utilisateurs** qui découlent du principe de loyauté : notamment, pertinence des critères de classement et de référencement mis en œuvre par la plateforme au regard de l'objectif de meilleur service rendu à l'utilisateur, définition des critères de retrait de contenus licites en termes clairs, accessibles à tous et non discriminatoires (**proposition n° 6**) ;

- d'organiser un **droit d'alerte** en matière de protection des données personnelles, sur le fondement du droit d'alerte « généraliste » reconnu par la loi du 6 décembre 2013 pour tout crime ou délit (**proposition n° 7**).

Les propositions portant sur les actions collectives sont les suivantes :

- création d'une **action collective** en matière de protection des données personnelles, permettant à certaines personnes morales agréées d'obtenir du juge une injonction de faire cesser des violations de la législation (**proposition n° 8**) ;

- mise en ***Open Data*** par la CNIL de toutes les **déclarations et autorisations** de traitements de données (**proposition n° 9**) ;

- développement de la **participation des utilisateurs** des plateformes **à l'élaboration des règles** définissant les contenus pouvant être mis en ligne sur leur site (**proposition n° 10**) ;

- attribution à la CNIL ou au Conseil national du numérique une mission permanente d'animation de la délibération collective sur les **enjeux éthiques** liés au numérique (**proposition n° 11**).

3.3. Redéfinir les instruments de la protection des droits fondamentaux et repenser le rôle des autorités publiques

• *En matière de protection des données personnelles*

Le cadre juridique de la protection des données personnelles a été défini alors que la circulation des données et leur valeur économique restaient limitées. L'intervention publique doit aujourd'hui assurer d'une part, la sécurisation juridique des usages des données, car c'est un facteur de développement de l'économie numérique, et d'autre part, un encadrement plus étroit des traitements présentant les risques les plus importants.

Afin de sécuriser juridiquement les usages présentant des risques limités pour les droits fondamentaux, les actions suivantes sont préconisées :

- maintenir sans ambiguïté dans la proposition de règlement européen la **liberté de réutilisation statistique des données personnelles**, quelle que soit la finalité initiale de leur traitement, en prévoyant pour seule condition que cette réutilisation soit entourée de garanties d'anonymat appropriées (**proposition n° 12**) ;

- renforcer le rôle de **conseil et d'accompagnement des responsables de traitement** par la CNIL et créer auprès d'elle une procédure de « rescrit données personnelles » (**propositions n° 13 et 14**) ;

- développer la corégulation avec les acteurs professionnels, en prévoyant une procédure d'homologation des codes de conduite, le respect d'un code homologué devant être l'un des critères retenus par l'autorité de contrôle pour ses décisions d'autorisation ou de sanction (**propositions n° 16, 17 et 18**).

Afin de proportionner l'encadrement au degré de risque du traitement, il convient de :

- créer pour les catégories de traitements présentant **les risques les plus importants** une **obligation de certification** périodique (complétant l'examen *a priori* par l'autorité de contrôle dans le cadre de la procédure de consultation préalable) par un organisme tiers indépendant et accrédité par l'autorité de contrôle (**proposition n° 19**) ;

- porter une attention particulière aux **transmissions de données personnelles d'une entité à une autre**, notamment en **codifiant dans la loi la jurisprudence** relative à la nullité des transactions portant sur des fichiers non autorisés ou non déclarés à la CNIL (**proposition n° 20**).

Le régime juridique des numéros d'identification devrait être revu, en mettant à l'étude la création d'un numéro national non signifiant (**proposition n° 21**) et dans l'immédiat, en élargissant les possibilités de recours au NIR dans le domaine de la santé et pour les autres usages (**proposition n° 22**).

Enfin, la protection des droits fondamentaux nécessite la mise en place d'outils de régulation de l'utilisation des algorithmes, notamment par l'exigence d'effectivité de **l'intervention humaine** dans le traitement des données (**proposition n° 23**) ou par l'observation de leurs résultats, notamment pour détecter des discriminations illicites, en renforçant à cette fin les moyens humains dont dispose la CNIL (**proposition n° 25**).

• *En matière de liberté d'expression*

Il conviendrait de prévoir une obligation pour les hébergeurs et les plateformes d'empêcher, durant un délai déterminé, la réapparition des contenus ayant fait précédemment l'objet de retrait ; cette obligation serait prononcée par l'autorité administrative (**proposition n° 28**).

L'existence de modalités spécifiques de contrôle des concentrations, qui complètent le contrôle général opéré par l'Autorité de la concurrence, est une garantie importante du pluralisme des médias. Cependant, en raison de la surabondance des contenus, les principales menaces pesant sur le libre choix des destinataires ne tiennent plus seulement à une concentration excessive, mais aussi à la fragilisation du modèle économique de la presse, alors que celle-ci demeure une source essentielle d'information de qualité. Il conviendrait de **revoir le contrôle de la concentration** dans les médias, et notamment les quotas et la mesure des bassins d'audience utilisés pour la limiter, propre à mieux garantir le pluralisme en tenant compte de la multiplicité des supports d'information (**proposition n° 30**).

• *Par le développement de la médiation*

Nombre de litiges liés à l'utilisation des technologies numériques, qu'ils portent sur les données personnelles, les atteintes à la réputation sur internet ou le retrait de contenus mis en ligne, peuvent être qualifiés de « petits litiges » :

leurs enjeux sont parfois significatifs pour les personnes concernées, mais les intérêts pécuniaires en cause sont le plus souvent limités. Les procédures juridictionnelles classiques sont peu adaptées au traitement de ces petits litiges, ce qui conduit nombre de personnes à renoncer à faire valoir leurs droits ; la médiation serait dans bien des cas plus adaptée (**proposition n° 31**).

3.4. Assurer le respect des droits fondamentaux dans l'utilisation du numérique par les personnes publiques

• *En matière d'ouverture des données publiques*

L'ouverture des données publiques, ou « *Open Data* », fait l'objet depuis 2011 d'une politique volontariste du gouvernement. Ce volontarisme politique, qui se traduit par l'affichage d'un principe d'ouverture par défaut aujourd'hui inscrit dans un instrument de droit souple, contraste avec la faiblesse des obligations prévues par le droit dur. L'inscription dans la loi d'une obligation de mise en ligne progressive de l'ensemble des bases de données détenues par l'administration présenterait plusieurs avantages, notamment celui d'étendre la politique d'*Open Data* aux collectivités territoriales, dont l'action en la matière est aujourd'hui inégale. Toutefois, la voie du droit souple apparaît plus appropriée pour promouvoir le développement de l'***Open Data***, notamment auprès de ces dernières. Une **charte d'engagements et de bonnes pratiques** pourrait donc être élaborée par l'État, les associations de **collectivités territoriales** et les représentants des utilisateurs des données, qui engagerait chaque organisme public adhérent à définir un programme d'ouverture de ses données publiques, à respecter des standards de qualité et à veiller à limiter les risques de réidentification (**proposition n° 32**). Ces risques seraient circonscrits par la définition de **bonnes pratiques d'anonymisation** et par la constitution au sein de chaque ministère un pôle d'expertise en matière d'anonymisation, *a priori* au sein du service statistique ministériel (**proposition n° 33**).

• *En matière de fichiers de police judiciaire*

Les fichiers de police judiciaire ont connu au cours des quinze dernières années une forte expansion liée notamment à l'allongement de la liste des infractions donnant lieu à enregistrement. Sans remettre en cause leur utilité pour les services de police, il apparaît souhaitable de renforcer les garanties entourant leur utilisation et de corriger certaines fragilités juridiques :

- Pour le fichier automatisé des empreintes digitales (FAED) et le fichier national automatisé des empreintes génétiques (FNAEG), il conviendrait de préciser les conséquences à tirer des décisions judiciaires (acquittement, non-lieu, relaxe, classement sans suite) (**proposition n° 34**). Pour le fichier « Traitement des antécédents judiciaires », il s'agit d'assurer la mise en œuvre effective des dispositions qui le régissent (**proposition n° 35**), les contrôles successifs de la CNIL ayant montré un taux très élevé d'erreurs et d'absence de prise en compte des suites judiciaires.

- La décision n° 2010-25 QPC du 16 septembre 2010 du Conseil constitutionnel devrait être mise en œuvre, en modulant la durée de conservation des données dans le FNAEG en fonction de la gravité de l'infraction et de l'âge de la personne au moment de l'enregistrement (**proposition n° 36**).

• *En matière de prévention des atteintes à la sécurité nationale*

Les **conséquences de l'arrêt *Digital Rights Ireland*** doivent être tirées en ce qui concerne **l'accès aux données de connexion collectées au titre de l'obligation de conservation systématique prévue par notre législation**, notamment en réservant l'accès à des fins de police judiciaire aux crimes et aux délits d'une gravité suffisante, en réexaminant les régimes prévoyant l'accès de certaines autorités administratives pour des finalités autres que la sécurité intérieure (notamment la HADOPI, l'ANSSI, l'administration fiscale, l'AMF) et en étendant, pour l'accès aux données de connexion, les règles spécifiques de protection qui bénéficient aux parlementaires, aux avocats, aux magistrats et aux journalistes en matière d'interceptions du contenu des communications (**proposition n° 38**).

Afin de satisfaire à l'exigence de prévisibilité de la loi issue de la jurisprudence de la CEDH, il conviendrait de définir par la loi le régime de l'interception des **communications à l'étranger,** en prévoyant les finalités de ces interceptions les garanties spécifiques bénéficiant aux résidents français et l'existence d'un contrôle d'une autorité administrative indépendante (**proposition n° 39**). Il conviendrait également de définir le régime juridique de l'utilisation par les services de renseignement, sur autorisation administrative, de certains moyens d'investigation spéciaux utilisant les techniques numériques aujourd'hui encadrés uniquement dans le cadre de la procédure judiciaire (déchiffrement, captation de données informatiques...) (**proposition n° 40**).

Il est proposé de faire de la CNCIS une autorité de contrôle des services de renseignement, dotée de moyens humains renforcés sur le plan quantitatif et qualitatif, avec des compétences de haut niveau en matière d'ingénierie des communications électroniques, d'informatique et d'analyse des données. Ses prérogatives devraient aussi être renforcées, par l'attribution de pouvoirs de contrôle sur pièces et sur place et d'un champ de compétences étendu aux interceptions opérées à l'étranger ainsi qu'à l'emploi des moyens d'investigations spéciaux (**proposition n° 41**). Les agents impliqués dans la mise en œuvre des programmes de renseignement auraient **un droit de signalement** à cette autorité administrative indépendante des pratiques manifestement contraires au cadre légal, selon des modalités sécurisées assurant la protection du secret de la défense nationale (**proposition n° 42**).

3.5. Organiser la coopération européenne et internationale

Un **socle de règles** applicables à tous les services dirigés vers l'Union européenne ou la France (selon que la règle est européenne ou nationale), quel que soit leur lieu d'établissement comprendrait (**proposition n° 43**) :

- la législation européenne relative à la protection des données personnelles, qui serait qualifiée à cette fin de « **loi de police** » au sens du droit international privé ;

- l'obligation de coopération des hébergeurs et des plateformes avec les autorités administratives et judiciaires, prévue par l'article 6 de la LCEN, dont le champ d'application territorial serait explicité ;

- le droit pénal, notamment les abus de la liberté d'expression, qui est déjà applicable à l'ensemble des sites, même établis à l'étranger mais destinés au public français.

En matière de protection des données personnelles, le *Safe Harbor* négocié avec les autorités américaines, devrait être réformé, en prévoyant un droit de regard des autorités européennes sur les contrôles et en renforçant les obligations de fond (**proposition n° 44**). En matière de lutte contre la cybercriminalité, un groupe d'action interétatique devrait être créé pour définir des recommandations et publier une liste d'États non coopératifs (**proposition n° 47**).

L'annonce de la fin du lien contractuel entre l'ICANN et le gouvernement américain ouvre des perspectives de réforme de la gouvernance d'internet, pour l'ICANN mais aussi pour les autres instances qui doivent être investies d'une mission d'intérêt général guidée par un « mandat » international. Le processus de réforme en cours doit être l'occasion de donner une traduction concrète à ces exigences. Il conviendrait de promouvoir la démocratisation de l'ICANN, notamment en créant une assemblée générale rassemblant l'ensemble des parties prenantes et pouvant mettre en cause la responsabilité du conseil d'administration. Le rôle des États devrait être renforcé, en permettant au comité représentant les gouvernements (GAC) d'adopter des résolutions contraignantes (**proposition n° 48**). Pour l'ensemble des instances, il conviendrait de diversifier la composition des organes de gouvernance d'internet, par des critères de sélection imposant une réelle diversité linguistique et géographique et la mise en place de stratégies d'influence de la France et de l'Union européenne (**proposition n° 49**). Une convention internationale relative aux libertés fondamentales et aux principes de la gouvernance d'internet devrait notamment énoncer les principes que s'imposeraient les signataires (**proposition n° 50**).

***

Lorsqu'il s'est engagé dans cette étude, le Conseil d'État savait qu'il était attendu sur le terrain de la défense des droits fondamentaux. Il savait aussi qu'il ne devait pas se borner à la seule position – au demeurant fort légitime – de gardien des droits des individus. Il a souhaité prendre en considération toutes les potentialités du numérique, tout particulièrement celles qui en font le vecteur d'une économie qui favorise l'innovation, la croissance et l'emploi.

Le Conseil d'État aurait manqué à son office et son étude annuelle, à son objectif, si n'avaient pas été concomitamment traités les deux aspects d'une même réalité : l'innovation numérique et le respect des droits fondamentaux des citoyens.

Le numérique et les droits fondamentaux

Introduction

Selon la déclaration adoptée le 24 avril 2014 par les participants à la conférence « *NetMundial* » de Sao Paulo, « *les personnes doivent jouir des mêmes droits fondamentaux lorsqu'elles ne sont pas connectées et lorsqu'elles sont en ligne* »[2]. Cette affirmation a la force de l'évidence. Sur internet, les personnes pratiquent l'ensemble des activités humaines : elles s'informent, s'expriment, nouent des relations personnelles, travaillent, commercent, consomment, étudient, diffusent ou consultent des œuvres, procèdent à des démarches administratives, se rassemblent par affinité de convictions, peuvent aussi se livrer à des activités délinquantes ou en être les victimes. Rien ne justifie qu'elles ne bénéficient pas sur internet des mêmes droits que ceux qui s'appliquent hors connexion. Le Conseil d'État l'avait d'ailleurs affirmé dès 1998 dans son étude thématique sur internet *et les réseaux numériques*[3], à une époque où la thèse selon laquelle internet échappait par nature au droit était encore vivace.

Pourtant, l'affirmation de l'applicabilité des droits fondamentaux ne suffit pas à épuiser le sujet. Le numérique[4], parce qu'il conduit à la mise en données et à la mise en réseau générale du monde, permet d'étendre et de valoriser les droits fondamentaux, mais il peut aussi les mettre en cause : non qu'il serait un phénomène négatif, mais il met en question leur contenu et leur régime. En effet, le numérique modifie les conditions d'exercice des droits fondamentaux. Il renforce la capacité des individus à jouir de certains droits, comme la liberté d'expression, la liberté d'entreprendre ou la liberté d'association. Mais il peut conduire aussi à les brider et il en fragilise d'autres, comme le droit de propriété intellectuelle dont il facilite la méconnaissance ou le droit à la vie privée qu'il affecte par la multiplication des traces laissées par les individus dans l'environnement numérique. Son effet sur

2. "*Rights that people have offline must also be protected online*"; la conférence mondiale des parties prenantes sur l'avenir de la gouvernance d'internet, dite « *NetMundial* », a rassemblé des représentants des États, des acteurs économiques, des ONG et les instances impliquées dans la gouvernance d'internet pour définir des principes communs relatifs à son évolution (cf. *infra* 1.4.2 et 2.3.3).

3. Études du Conseil d'État, La documentation Française, 1998.

4. La présente étude a choisi de retenir le terme sous la forme de l'adjectif substantivé, car il est passé dans le langage courant (V. par exemple, *Le Petit Larousse* édition 2000), plutôt que l'expression « *les technologies numériques* ». Le Conseil d'État définit dans cette étude le numérique comme « *la représentation de l'information ou de grandeurs physiques (images, sons) par un nombre fini de valeurs discrètes, le plus souvent représentées de manière binaire par une suite de 0 et de 1* » (cf. *infra* 1.1.1).

chaque droit fondamental est souvent ambivalent. Ainsi, le numérique favorise la « *cybercriminalité* », expression qui recouvre à la fois des formes traditionnelles de délinquance employant les moyens numériques (comme les escroqueries) et des nouvelles menaces pour la sécurité des personnes et des biens (comme l'atteinte aux systèmes d'information), mais il renforce aussi les moyens d'action des forces de police ; il affecte le droit d'auteur mais est un vecteur d'accès aux connaissances et à la culture. Pour certains, le numérique inviterait même à la découverte de nouveaux droits, tels que le « *droit à l'oubli* », le « *droit à la déconnexion* » ou le « *droit au silence des puces* » ou, à l'inverse, à constater l'obsolescence du droit à la vie privée ou du droit d'auteur. Somme toute, si le numérique est indubitablement soumis aux droits fondamentaux, il rétroagit aussi sur eux.

L'étude annuelle du Conseil d'État pour 2014, consacrée au numérique et aux droits fondamentaux, intervient à un moment particulier, où le phénomène prend une nouvelle dimension. Un triple basculement se manifeste, dans les innovations technologiques, dans l'économie et dans l'appréhension du numérique par la société. Les interrogations sur les rapports du numérique aux droits fondamentaux se trouvent de ce fait renouvelés renforcées.

Le premier basculement a trait au changement de nature des innovations liées au numérique. Au cours des dernières décennies, celles-ci étaient restées cantonnées aux « *technologies de l'information et de la communication* » (TIC), expression souvent employée comme un équivalent au numérique. La portée réelle de ces innovations a parfois fait l'objet d'un certain scepticisme. Selon la formule de Peter Thiel, un des fondateurs du service de paiement en ligne *PayPal* et aujourd'hui l'un des principaux acteurs du capital-risque : « *Nous voulions des voitures volantes, et nous n'avons eu que 140 caractères*[5] ». Aujourd'hui, les innovations liées au numérique se déploient cependant bien au-delà du champ des TIC. Elles sont motrices dans les progrès de la robotique, de l'intelligence artificielle ou des objets connectés. Si les voitures volantes ne sont pas encore d'actualité, les voitures sans chauffeur roulent déjà sur les routes du Nevada ou du centre-ville de Lyon[6] ; d'autres avancées techniques qui, il y a encore quelques années, n'avaient cours que dans les ouvrages de science-fiction, permettent aujoud'hui de produire des logiciels de traduction orale en temps réel ou des robots en mesure de percevoir et de réagir aux émotions manifestées par les êtres humains[7].

De même, sur le plan économique, le numérique déploie son pouvoir de transformation bien au-delà de ses premiers secteurs d'implantation. La presse, les industries culturelles, le marketing et la finance ont été bouleversés dès les années 2000 ; aujourd'hui, l'automobile, l'hôtellerie, le transport de personnes, la santé,

---

5. "*We wanted flying cars, instead we got 140 characters*" : il s'agit d'une allusion au réseau social *Twitter*, où les messages sont limités à 140 caractères. Cf. G. Packer, "*No death. No taxes. The libertarian futurism of a Silicon Valley billionaire*", *The New Yorker*, 28 novembre 2011.

6. Il s'agit de la voiture sans chauffeur développée par *Google* et de la voiture *Navia* conçue par la société *Induct*.

7. Il s'agit respectivement du *Skype Translator* du groupe *Microsoft* et du robot *Pepper* de la société *Aldebaran*.

l'énergie et même l'agriculture voient leur économie modifiée par l'utilisation d'un volume toujours croissant de données (phénomène souvent désigné par l'expression de « *Big Data* ») et les nouvelles possibilités d'interaction avec les clients permises par la généralisation de l'internet mobile. De nouveaux acteurs économiques y acquièrent en l'espace de quelques années un pouvoir considérable, remettant en cause les positions les mieux établies. En raison du caractère transnational de leur activité, de leur capacité à susciter l'adhésion d'un nombre massif de clients et de la fréquente difficulté de leur insertion dans la réglementation existante, ils lancent un défi au pouvoir de régulation des États et brouillent certains principes établis du droit, tel que celui de la territorialité de la norme.

Enfin, la société se modifie rapidement dans son appréhension du phénomène numérique. Internet et le smartphone se sont diffusés dans les foyers plus vite que toute autre innovation dans le passé, modifiant les relations sociales et jouant un rôle souvent intense dans la vie des adolescents. Mais c'est dans le débat public que la transformation est la plus récente et la plus marquée : des sujets tels que le *Big Data*, les objets connectés ou la neutralité du *net*, souvent cantonnés hier aux gazettes spécialisées, trouvent aujourd'hui leur place dans les unes des quotidiens d'information générale et dans les émissions télévisées destinées au grand public. Sur un terrain déjà fertile en interrogations[8], les révélations intervenues depuis juin 2013 sur la surveillance des communications opérée par les États-Unis et d'autres États ou la découverte du rôle joué par internet dans le recrutement de volontaires par des organisations jihadistes ont sans conteste été des moments de cristallisation dans l'émergence des sujets de société liés au numérique. Au regard des libertés publiques, de la confiance dans l'utilisation et la fréquentation des réseaux sociaux et d'internet en général, il est souvent entendu et communément admis que « *rien ne sera comme avant l'affaire Snowden* ». Encore faut-il que cette prise de conscience soit effective et partagée et débouche sur des mesures à la hauteur du problème soulevé.

Face à ce triple basculement, le droit du numérique est remis en question, y compris dans sa dimension la plus importante, celle de la protection des droits fondamentaux. Il est tour à tour accusé d'être impuissant à protéger les individus ou de mettre trop d'entraves à l'économie numérique, d'être trop lent à prendre les mesures de protection attendues ou, au contraire, trop instable pour favoriser durablement l'innovation. Les rapports sectoriels et les propositions de réforme sectoriels portant sur certaines politiques publiques ou sur certaines branches du droit se multiplient, par exemple dans les domaines de la culture, la santé, l'éducation, la cybersécurité, l'ouverture des données publiques ou le renseignement.

L'ambition de l'étude du Conseil d'État n'est pas de se substituer aux travaux sectoriels très approfondis qui ont été conduits ces dernières années. Elle consiste plutôt à proposer une approche générale afin de répondre à la question suivante : face aux bouleversements suscités par le numérique, dans quelle mesure la protection des droits fondamentaux doit-elle être repensée ? Les libertés fondamentales les

8. Comme en témoigne par exemple l'intensité des débats suscités en France par la loi du 12 juin 2009 favorisant la diffusion et la protection de la création sur internet, dite loi HADOPI.

plus concernées, notamment la liberté d'expression, la liberté d'entreprendre, le droit à la vie privée et à la protection des données personnelles, le droit à la sécurité et le droit de propriété intellectuelle sont particulièrement étudiées. Les réponses les plus pertinentes aux contradictions du numérique naissent d'ailleurs de la nécessaire conciliation de ces différentes libertés fondamentales. L'étude est bien sûr attentive aux risques que présente le phénomène numérique, mais elle n'entend pas méconnaître le rôle positif de ce dernier dans l'exercice des libertés ni sa contribution à la réforme des politiques publiques, à l'innovation et à la croissance économique. Les mesures prises pour parer aux risques ne doivent pas contrarier les effets bénéfiques du numérique. Le but de l'étude n'est pas de proposer des protections supplémentaires contre le numérique, mais de faire en sorte que les dangers dont il est porteur n'en étouffent pas le potentiel libérateur.

Plus encore que dans les études annuelles précédentes, le Conseil d'État a cherché à rassembler et à croiser les points de vue. 70 auditions ont été conduites auprès d'entreprises de l'économie numérique, d'associations, d'universitaires, d'experts, de responsables des ministères et des autorités administratives indépendantes (AAI) compétentes. Les échanges avec le Parlement ont été particulièrement intenses, puisqu'outre les rencontres avec le président de la commission des lois de chacune des deux assemblées parlementaires et l'audition de deux députés, les rapporteurs de l'étude du Conseil d'État ont eux-mêmes été auditionnés dans le cadre de deux missions d'information du Sénat[9]. Pour conduire des échanges plus suivis et plus approfondis que ceux auxquels peut donner lieu une audition, le Conseil d'État a créé un « *groupe de contacts* », composé de personnalités du secteur public, de l'université, de l'économie numérique et des AAI, qui a été réuni à quatre reprises pour donner le point de vue de ses membres lors des différentes phases de l'avancement des travaux. Compte tenu du rôle central joué par l'Union européenne, deux déplacements ont été effectués à Bruxelles auprès des institutions de l'Union, et le député européen rapporteur de la proposition de règlement sur la protection des données personnelles a été auditionné à Paris. Enfin, une grande place a été donnée au droit comparé, l'étude ayant bénéficié des auditions de plusieurs experts, des recherches de la cellule de droit comparé du Conseil d'État ainsi que de l'analyse de cinq postes diplomatiques (Allemagne, Brésil, Chine, Corée du sud et États-Unis).

Au terme de cette analyse, il apparaît clairement que l'enjeu n'est pas de compléter la liste des droits fondamentaux. Il n'est pas nécessaire de proclamer, dans une nouvelle charte constitutionnelle, des droits fondamentaux qui seraient propres à l'ère numérique ; les droits existants, qui ont été énumérés ci-dessus, conservent toute leur pertinence. Il n'est pas souhaitable non plus de changer radicalement la conception du droit à la protection des données personnelles, en transformant le droit personnel qu'il a toujours été depuis la loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés en un droit patrimonial. En revanche, le mode de protection des droits fondamentaux appelle de profondes révisions.

9. Mission commune d'information « Nouveau rôle et nouvelle stratégie pour l'Union européenne dans la gouvernance mondiale de l'Internet » ; Mission d'information sur l'*Open Data* et la protection de la vie privée.

En premier lieu, l'effectivité de l'intervention publique passe par l'affirmation du champ d'application territorial de la règle de droit, que celle-ci soit nationale ou européenne. Il ne sert à rien d'édicter des lois protectrices, si elles ne sont pas applicables aux principaux acteurs du numérique ou si les sanctions de leur violation sont trop faibles pour être dissuasives. Compte tenu du caractère transnational d'internet, le champ d'application territorial des règles de droit les plus fondamentales dans la protection des internautes et de l'ordre public doit englober les acteurs extérieurs au territoire national ou européen. Pour ces règles, dont l'étude se propose de définir le socle, le principe d'application de la loi du pays de destination, et non du pays d'origine, doit prévaloir. Le rappel à la loi et au règlement n'est pas exclusif d'un recours plus étendu au droit souple, selon les voies préconisées dans l'étude annuelle de 2013 du Conseil d'État[10] : les pouvoirs publics doivent tout à la fois davantage inciter à des comportements responsables, davantage sanctionner les atteintes aux droits fondamentaux.

En deuxième lieu, le droit doit prendre la mesure du rôle joué par les nouveaux acteurs de l'économie numérique, dont certains ont acquis une place considérable, tant en termes de pouvoir de marché que de prescription des contenus. L'étude du Conseil d'État invite à faire entrer pleinement dans le droit positif ces deux réalités centrales de la société numérique contemporaine que sont les plateformes et les algorithmes. Elle propose notamment de consacrer un principe de loyauté des plateformes, qui serait le pendant du principe de neutralité des opérateurs de communications électroniques.

En troisième lieu, le Conseil d'État appelle les pouvoirs publics à renforcer le pouvoir des personnes, agissant de manière individuelle ou collective, afin d'en faire des gardiens efficaces de leurs propres libertés. La loi, qu'elle soit nationale ou européenne, doit prêter main forte aux individus pour rééquilibrer leur relation avec les grands acteurs du numérique. Ceci passe certainement par une promotion des technologies renforçant la maîtrise de la personne sur l'utilisation de ses données et par l'organisation de la délibération collective sur les enjeux éthiques liés au numérique.

Étudier le numérique et les droits fondamentaux, c'est en dernière analyse s'interroger sur le rôle de la puissance publique. Celle-ci est mise au défi dans sa capacité à garantir les droits fondamentaux, à protéger la sécurité nationale tout en respectant elle-même ces droits. Il lui revient aussi de définir une stratégie économique pertinente pour que le numérique concoure à la prospérité de la Nation. Pour relever ce défi, la puissance publique doit s'allier avec les individus, avec « la multitude » selon l'expression désormais consacrée[11]. Elle doit aussi s'exercer, chaque fois que cela est nécessaire, au niveau européen. Le numérique suscite l'adhésion en masse du public ; ce n'est pas en cherchant à entraver cette adhésion que la puissance publique parviendra à en limiter les risques, mais en donnant aux individus le pouvoir de veiller à la défense de leurs droits. Les enjeux

10. Conseil d'État, *Le droit souple*, La documentation Française, 2013.

11. N. Colin et H. Verdier, *L'âge de la multitude. Entreprendre et gouverner après la révolution numérique*, Armand Colin, 2012.

du numérique se jouent à l'échelle mondiale : l'Union européenne, forte de ses 400 millions d'internautes, est bien plus à même d'imposer ses règles et de dialoguer avec les États-Unis et les autres grands espaces juridiques que chacun de ses États membres.

La réflexion que propose le Conseil d'État dans cette étude sera conduite selon la progression suivante. Tout d'abord, la complexité du sujet nécessite un état des lieux qui montre comment le numérique a déjà modifié les conditions d'exercice des libertés fondamentales (I). Puis, l'étude présente la problématique générale qui sous-tend la réflexion du Conseil d'État et expose en quoi l'ambivalence intrinsèque du numérique et la façon de concilier les tensions qui en résultent implique de repenser la protection des droits fondamentaux (II). Enfin, elle formule 50 propositions dont le fil directeur est la protection des droits fondamentaux en renforçant le pouvoir des individus sans, pour autant, nuire au potentiel d'innovation du numérique (III).

L'essor du numérique a suscité la reconnaissance de nouveaux droits fondamentaux et modifié leurs conditions d'exercice

Envisager la manière dont le numérique affecte les droits fondamentaux, c'est déjà postuler son importance et sa spécificité par rapport à d'autres mutations technologiques. L'automobile, la télévision ou les antibiotiques ont ouvert à leur apparition de nouvelles perspectives à la liberté d'aller et de venir, à la liberté de communication et au droit à la santé, et ont pu appeler des législations et des réglementations spécifiques ; ils n'ont pas pour autant modifié le contenu de ces droits fondamentaux. Le numérique est différent : il ne s'agit pas d'une simple innovation mais d'une série de mutations technologiques faisant système, qui entraînent de profondes transformations économiques et sociales dans l'ensemble des activités humaines. En outre, la succession très rapide de ces mutations au cours des vingt dernières années laisse augurer que le phénomène est encore loin d'avoir atteint toute son ampleur.

L'exposé des transformations techniques, économiques et sociales (1.1) est un préalable nécessaire pour comprendre comment l'essor du numérique a conduit à la consécration de deux nouveaux droits fondamentaux, le droit à la protection des données personnelles et le droit d'accès à internet (1.2), tout en modifiant les conditions d'exercice de plusieurs autres droits fondamentaux (1.3). Sans échapper à la puissance de l'État, il interpelle celui-ci de manière inédite (1.4). Le numérique doit en conséquence être pensé à la fois comme un espace de libertés et un enjeu stratégique (1.5).

1.1. L'essor du numérique entraîne des mutations techniques, économiques et sociales

Pour en prendre la juste mesure, il convient d'éviter deux acceptions trop restrictives du phénomène numérique. Le numérique ne se réduit pas à internet, mais forme un système d'innovations techniques dont internet permet la mise en réseau ; le numérique n'est pas qu'un système d'innovations techniques, mais aussi un ensemble de transformations sociales et économiques, les trois dimensions s'alimentant l'une l'autre. Par la formule « le numérique », on désignera donc dans cette étude non seulement le phénomène technique, mais l'ensemble de ces mutations.

1.1.1. Des révolutions techniques : la mise en réseau des machines, la mise en données du monde

Le numérique se définit comme la représentation de l'information ou de grandeurs physiques (images, sons) par un nombre fini de valeurs discrètes[12], le plus souvent représentées de manière binaire par une suite de 0 et de 1. Il s'oppose ainsi à l'analogique, dans lequel les signaux sont véhiculés sous la forme d'ondes continues.

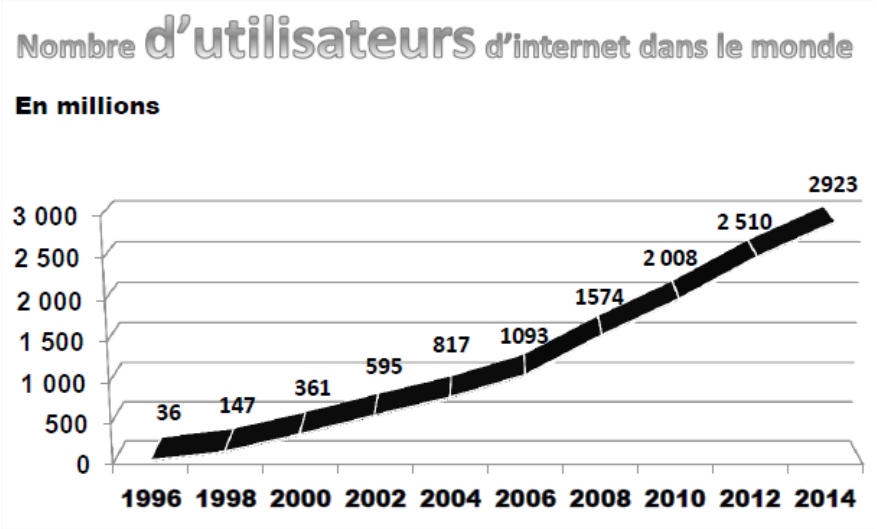
Ainsi formulée, cette définition peut sembler anodine, de même que nombre d'applications du numérique dont nous sommes familiers dans notre vie quotidienne, comme le compact-disc, l'informatique de bureau ou la photographie numérique. Le passage de l'analogique au numérique a ouvert la voie à des applications utiles ; mais pourquoi et en quoi ce changement serait-il porteur de sens pour les droits fondamentaux ? La définition du numérique porte pourtant en germe l'ensemble des transformations qui vont être exposées. En effet, la puissance transformatrice du numérique tient à sa capacité à exprimer des réalités disparates (sons, images, textes, phénomènes naturels, comportements humains, processus industriels....) dans un langage commun universel, fait de combinaisons de 0 et de 1, ouvrant la possibilité de les traiter de manière systématique et de les mettre en relation. Le philosophe Bernard Stiegler qualifie ce processus de « grammatisation » du réel, qu'il caractérise ainsi : « *c'est un processus de description, de formalisation et de discrétisation des comportements humains (calculs, langages et gestes) qui permet leur reproductibilité* »[13].

Les mutations techniques qui constituent le phénomène numérique peuvent être regroupées en deux tendances : la progression exponentielle de la puissance de calcul, de stockage et de reproduction ; la mise en réseau généralisée permise par

12. En mathématiques, on appelle ensemble discret un ensemble dont tout élément possède un voisinage dans lequel aucun autre élément n'est présent. En termes imagés, tous les éléments d'un ensemble discret sont séparés par des « trous ». L'ensemble des nombres entiers est discret, à la différence de l'ensemble des fractions rationnelles ou de l'ensemble des nombres réels.

13. http://arsindustrialis.org/grammatisation

internet, dont le nombre d'utilisateurs est estimé fin 2014 à près de 3 milliards, un nouveau milliard d'utilisateurs étant attendu pour 2017[14]. Ces deux tendances combinées ouvrent la voie à l'explosion des données (*Big Data*) et à de nouvelles formes d'interactions entre machines et êtres humains.



Source : graphique : Conseil d'État, section du rapport et des études ; données : Internet World Stats et International Telecommunication Union

La progression exponentielle de la puissance de calcul, de stockage et de reproduction

La « loi de Moore » est une prédiction formulée en 1965 par Gordon Moore, l'un des cofondateurs de la société Intel, dans un article de la revue *Electronics*[15]. Il avait relevé que, depuis l'invention des semi-conducteurs, le nombre de transistors sur une puce de silicium de prix constant doublait tous les ans, et prédisait que cette progression exponentielle se poursuivrait. Plusieurs variantes de cette loi ont été formulées, différant par le rythme de la progression (tous les deux ans, tous les dix-huit mois) ou par la grandeur dont la croissance est mesurée (« fréquence d'horloge » du processeur exprimée en hertz, puissance, etc.). La « loi de Moore » n'est pas une loi physique s'expliquant par une relation de causalité, mais un constat empirique qui s'explique par une succession d'innovations techniques dans les modes de fabrication des processeurs. Toujours est-il que conformément à la prédiction, la puissance de calcul des ordinateurs a bien connu jusqu'ici la croissance exponentielle annoncée.

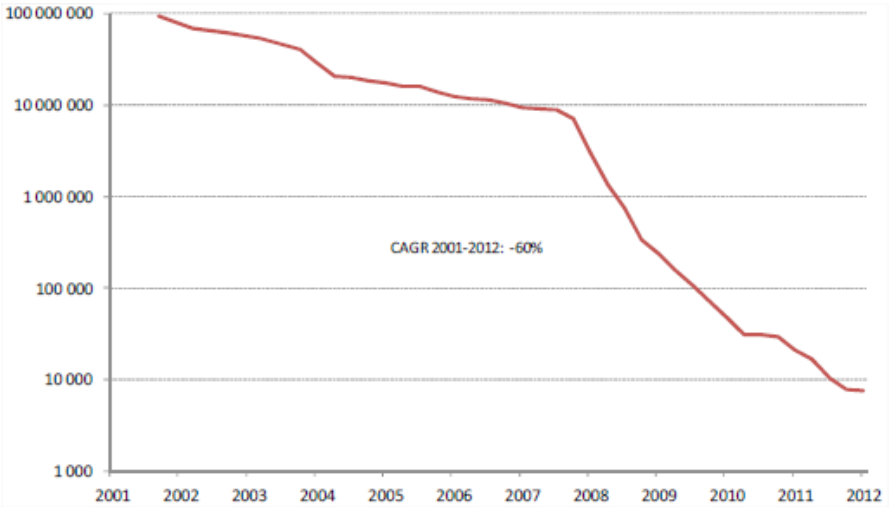
Les implications de la « loi de Moore » sont considérables. Il est commun de relever qu'un smartphone dispose d'une **puissance de calcul** supérieure à celle des supercalculateurs les plus performants d'il y a quelques décennies. Certaines

14. « The Next Billion Internet Users. What Will They Look Like ? », www.internetserviceproviders.org, août 2013.

15. Gordon E. Moore, « Cramming More Components Onto Integrated Circuits », *Electronics*, vol. 38, avril 1965.

applications de cette vitesse inédite permettent sans doute de mieux prendre la mesure du progrès accompli. Le séquençage d'un génome humain, lancé en 1987 dans le cadre du consortium international de recherche *Human Genome Project*, était initialement un projet d'une ambition démesurée, nécessitant l'implication de généticiens du monde entier et qui n'a été achevé qu'en 2003, pour un coût total de 2,7 milliards de dollars. Le coût du séquençage est tombé en 2012 à moins de 10 000 dollars[16], et des projets offrant un « génome à 1 000 dollars »[17], ainsi à la portée de nombreux individus, ont été annoncés en 2013.

Coût du séquençage par génome, 2001-2011, en USD (échelle logarythmique)



Source: OCDE basé sur les travaux de l'United States National Human Genome Research Institute (www.genome.gov/sequencingcost), OECD (2013), "Exploring Data-Driven Innovation as a New Source of Growth: Mapping the Policy Issues Raised by "Big Data"", OECD Digital Economy Papers*, No. 222, OECD Publishing. http://dx.doi.org/10.1787/5k47zw3fcp43-en.*

Les capacités de stockage ont suivi le même rythme que la puissance de calcul des ordinateurs. Le coût d'un gigaoctet de stockage sur un disque dur est passé de 56 dollars en 1998 à 0,05 dollars en 2012, soit une diminution de 40 % par an[18]. Par son ampleur, cette chute des prix a bouleversé l'économie du stockage. Alors que les entreprises et les administrations étaient dans le passé contraintes, pour des raisons économiques, de procéder régulièrement à un tri et à un effacement des données générées par leur activité, le coût devenu négligeable du stockage ouvre la possibilité d'une conservation illimitée. Les particuliers en font aussi l'expérience : astreints dans un passé encore proche à la corvée du classement et de la suppression des messages ou des fichiers, ils ont aujourd'hui accès à des services en ligne qui leur offrent une capacité de stockage dépassant les besoins de la plupart des individus.

16. OCDE, *Exploring Data-Driven Innovation as a New Source of Growth*, juin 2013.
17. H. Morin, « Le génome humain à 1 000 dollars », *Le Monde*, 1er janvier 2013.
18. OCDE, 2013, précité.

Ouvrant des perspectives inédites de calcul et de conservation de l'information, le numérique permet aussi une **reproduction illimitée** de celle-ci. Les supports analogiques présentaient à cet égard un triple défaut : le coût, le temps de reproduction et la perte de qualité à chaque copie successive. Le numérique permet aujourd'hui une copie gratuite, tendant à l'instantanéité et sans dégradation quel que soit le nombre de reproductions.

La mise en réseau généralisée : internet et l'informatique en nuage (« cloud computing »)

Internet tel que nous le connaissons repose sur des choix d'architecture originaux, faits dès les premières décennies de sa gestation et qui ont perduré depuis, montrant ainsi une robustesse et une capacité d'adaptation sans doute insoupçonnables même par leurs concepteurs.

- Le premier de ces choix est celui de la « commutation de paquets » : il s'agit d'un mode d'acheminement de l'information dans lequel les messages sont découpés en paquets et transmis selon un parcours non déterminé à l'avance, seule la destination finale étant connue ; les paquets transitent par les « nœuds » du réseau, qui les acheminent vers le nœud suivant en fonction des capacités disponibles, et ce jusqu'à l'arrivée à la destination. La « commutation de paquets » s'oppose à la « commutation de circuits », qui est celle employée par exemple dans les réseaux téléphoniques et qui implique la réservation de bout en bout d'une ligne pour toute la durée de la communication. Elle présente deux avantages par rapport à celle-ci : une meilleure résilience du réseau en cas de dysfonctionnement d'une de ses parties, par exemple dans une situation de conflit armé ; une meilleure rentabilité pour les échanges de données, la commutation de paquets n'impliquant pas, à la différence de la commutation de circuits, la réservation d'une ligne pendant toute la durée de la communication (un même « nœud » peut recevoir simultanément des paquets issus de communications différentes). Les premières recherches sur la commutation de paquets ont été conduites au début des années 1960 par la *Defence Advanced Reasearch Projets Agency* (DARPA), une agence du ministère de la défense américain. On peut également mentionner le rôle joué par le projet Cyclades de l'Institut de recherche en informatique et en automatique (IRIA, aujourd'hui INRIA), conduit par le chercheur français Louis Pouzin ; celui-ci est notamment reconnu comme étant l'inventeur du « datagramme »[19], le procédé consistant à découper les données transmises en paquets pouvant suivre des chemins différents pour arriver à leur destination.

- Le protocole de communication TCP/IP (*Transmission Control Protocol / internet Protocol*), défini en 1973 par Robert E. Kahn, ingénieur de la DARPA, et Vinton Cerf, chercheur à Stanford, a été construit pour permettre une architecture ouverte, c'est-à-dire pour que chaque réseau puisse être connecté à l'interréseau sans qu'il soit besoin qu'il ait été conçu pour cela. Il repose sur quatre règles de base : un réseau n'a pas besoin d'être modifié pour être connecté à internet ; les communications se font selon le principe du « meilleur effort » (*best effort*), sans garantie de délai

19. V. par ex. Wired, « Say Bonjour to the Internet's Long-Lost French Uncle », par Cade METZ, 1er mars 2013, http://www.wired.com/2013/01/louis_pouzin_internet_hall/.

ou de qualité ; les machines utilisées dans les nœuds d'interconnexion, appelées routeurs, se contentent d'acheminer le paquet au nœud suivant en vue de le rapprocher de sa destination finale, et sont aveugles au contenu du message transmis ; il n'existe pas de contrôle centralisé du fonctionnement de l'internet.

- Selon la formule employée par un rapport du Commissariat général à la stratégie et à la prospective (CGSP), « *l'internet que nous connaissons est né au début des années 1990, forgé par la convergence d'une innovation technique, le protocole IP et ses équipements de routage, et d'une innovation d'usage, le lien hypertexte* »[20]. En d'autres termes, internet résulte de la combinaison d'un mode de communication entre des machines, le protocole TCP/IP, et d'un instrument de mise en relation des contenus proposés par ces machines, le lien hypertexte, le réseau constitué par l'ensemble de ces liens étant dénommé « *world wide web* ». Le lien hypertexte a été inventé par Tim Berners-Lee, un chercheur britannique du Centre européen de recherche nucléaire (CERN), qui est aussi l'auteur de l'expression « *world wide web* ».

Ces quelques choix et innovations structurants étaient porteurs des évolutions observées depuis lors. Le caractère ouvert et décentralisé de l'architecture d'internet lui a permis de supplanter les initiatives concurrentes de mise en réseau dans les années 1970 et 1980, d'intégrer dans le réseau de nouveaux types d'équipements terminaux (les ordinateurs personnels dans les années 1980, les téléphones mobiles dans les années 2000, les objets connectés dans les années 2010) et de connaître ainsi une expansion quantitative continue. Le principe du « meilleur effort », bien que peu séduisant en apparence en raison de l'absence de garanties de qualité et de délai, a montré sa robustesse et sa rentabilité. La généralisation des liens hypertextes a permis d'autres innovations d'usage, telles que les navigateurs internet (des logiciels qui permettent d'accéder aux contenus associés à une adresse internet, en interrogeant les serveurs correspondants *via* le protocole HTTP) et les moteurs de recherche (des robots qui interrogent le contenu de l'ensemble des sites internet à partir de mots-clés fournis par l'utilisateur, puis classent les résultats obtenus en fonction d'un ordre de pertinence déterminé par leur algorithme). Ces applications permettent à chaque utilisateur d'internet d'exploiter la masse des ressources disponibles de manière pertinente, rendant ainsi soutenable la croissance de cette masse.

Par la mise en réseau généralisée, internet permet de dissocier la propriété et l'utilisation des moyens informatiques. Un particulier, une entreprise ou une administration ne sont plus tenus de posséder le matériel informatique et les logiciels correspondant à leurs besoins ; ils peuvent utiliser les ressources détenues par des tiers, accessibles *via* internet, et n'ont plus besoin que du seul équipement terminal (ordinateur, téléphone, tablette) permettant d'y accéder. La possibilité de dissociation est inhérente à internet et le grand public est familier depuis plus d'une décennie de certaines de ces applications : des services de messagerie électronique sont accessibles par internet (c'est-à-dire sans que le particulier ait à installer de logiciel ni à stocker les messages sur ses équipements) depuis la fin des années 1990 et des services de stockage et de partage de photographies depuis le début des années 2000.

20. CGSP, « La dynamique d'internet. Prospective 2030. », *Études*, n° 1, mai 2013.

Le phénomène prend cependant une nouvelle dimension depuis quelques années. L'accroissement du débit des connexions à internet (par la fibre optique pour les connexions fixes et la quatrième génération des connexions mobiles) et l'explosion du volume des données (cf. le point suivant) ont ouvert la voie à ce qu'on pourrait qualifier d'industrialisation de la dissociation, et qui est généralement désignée par l'expression de « *cloud computing* », ou « informatique en nuage ». Selon la définition couramment reprise du *National Institutes for Standards and Technology* (NIST), un organisme de normalisation américain, l'informatique en nuage est un système d'accès par le réseau à des ressources informatiques mutualisées, mobilisables et configurables à la demande. Ces ressources sont fournies par des entreprises spécialisées et peuvent être des logiciels, des équipements informatiques, des plateformes de développement d'applications ou encore des capacités de stockage de données[21]. On distingue le « cloud privé », dans lequel des ressources du prestataire sont dédiées à l'utilisateur, du « cloud public », dans lequel les ressources sont mutualisées ; une même ressource peut alors servir aux besoins de plusieurs utilisateurs, le prestataire optimisant en permanence l'allocation de ses moyens.

Plusieurs intérêts économiques sont attendus de l'informatique en nuage. Elle permet de dégager des économies d'échelle, les entreprises prestataires parvenant à une plus grande efficacité dans l'utilisation des ressources informatiques grâce à leur spécialisation. Elle dispense les utilisateurs de consentir de lourds investissements pour acquérir les moyens informatiques nécessaires à leur activité, facilitant ainsi la création d'activités et l'innovation ; les utilisateurs peuvent aussi plus aisément moduler leurs moyens informatiques en fonction de l'évolution de leurs besoins, faisant ainsi face aux pics d'activité et évitant les surcapacités. Ces avantages conduisent les pouvoirs publics à promouvoir le développement de l'informatique en nuage[22].

Pour autant, l'informatique en nuage soulève des questions délicates et pour certaines inédites, notamment sur le plan juridique. La loi applicable peut être malaisée à déterminer en raison de la difficulté à localiser physiquement les ressources informatiques utilisées ou les données hébergées (cf. *infra* 1.4 pour des développements plus approfondis) : en effet, les modalités de gestion de l'informatique en nuage, reposant sur une optimisation permanente, conduisent à faire varier fréquemment les serveurs utilisés pour répondre aux besoins d'un utilisateur, voire à diviser le stockage d'une même donnée entre plusieurs serveurs, pouvant être situés sur deux continents différents… La responsabilité du prestataire en cas de perte de données ou de dysfonctionnement des ressources

21. Ces types de services d'informatique en nuage sont communément désignés par les expressions et les acronymes de « *Software as a Service* » (SaaS), « *Infrastructure as a Service* » (IaaS), « *Platform as a Ser*vice » (PaaS) et *« Data as a Service* » (DaaS).

22. Au niveau européen, la Commission européenne a défini une stratégie en la matière : cf. « Libérer tout le potentiel de l'informatique en nuage en Europe », communication du 27 septembre 2012, COM(2012) 529. En France, le développement d'une offre nationale d'informatique en nuage est soutenu par le programme d'investissements d'avenir et fait partie des 34 priorités définies dans le cadre de la « Nouvelle France industrielle » en septembre 2013.

informatiques appelle des précisions[23]. Les risques pour la sécurité des données, notamment lorsqu'il s'agit de données sensibles pour des enjeux de vie privée ou de secret industriel, peuvent être malaisés à évaluer ; ils sont en partie liés à la question de la loi applicable, les lois d'États tiers pouvant offrir un niveau variable de protection des données personnelles.

L'explosion des données ou « Big Data »

La croissance combinée du nombre d'utilisateurs d'internet et des débits de connexion a conduit à une explosion du volume des données transitant sur les réseaux. En 2012, le trafic mensuel a été de 43 exaoctets par mois, c'est-à-dire 43 milliards de milliards d'octets (10^{18}) ; c'est 20 000 fois plus qu'en 1996. Le taux de croissance du trafic est encore de 40 % par an, ce qui équivaut à un quasi doublement tous les deux ans. La montée en puissance de « *l'internet des objets* » pourrait en outre donner un essor accru à cette expansion, les données transmises par les objets connectés s'ajoutant à celles issues des activités des internautes humains.

La capacité à exploiter cette masse de données pour produire des applications ayant une utilité économique ou sociale s'est considérablement développée ces dernières années. En effet, ce n'est qu'au cours de cette période que des solutions permettant d'exploiter des données hétérogènes (textes, images, données de connexion, données de localisation, etc.) et non structurées sous forme de base de données ont été développées. L'expression « *Big Data* » désigne ainsi non seulement l'expansion du volume des données mais aussi celle de la capacité à les utiliser. Les enjeux associés au *Big Data* sont parfois exposés[24] en utilisant la formule des « *5 V* » : le *volume*, en raison de la masse des données à exploiter ; la *variété*, du fait de leur hétérogénéité ; la *vélocité*, certaines applications reposant sur une exploitation des données en temps réel ; la *véracité*, le manque de fiabilité des données exploitées pouvant remettre en cause les conclusions qui en sont tirées ; la *valeur* attendue de leur exploitation.

Les applications du *Big Data* sont multiples et en constant développement. On ne mentionnera ici que quelques illustrations significatives[25].

- L'analyse de l'activité sur internet peut fournir des **indicateurs avancés et fiables** pour de nombreuses tendances. Depuis 2008, l'entreprise *Google* utilise les requêtes formulées sur son moteur de recherche pour détecter les épidémies de grippe avec dix ou quinze jours d'avance sur les réseaux classiques de veille sanitaire, avec des résultats probants jusqu'en 2012[26]. Le « *Billion Price Project* », une initiative

23. La Commission européenne a lancé un groupe de travail pour élaborer des conditions-types « *sûres et équitables* », destinées à servir de modèle dans les contrats entre les utilisateurs et les prestataires d'informatique en nuage.

24. Cf. par ex. CGSP, « Analyse des big data. Quels usages, quels défis ? », *Note d'analyse*, n° 8, novembre 2013.

25. Cf. notamment OCDE, « Exploring Data-Driven Innovation as a New Source of Growth », *OECD Digital Economy Papers*, n° 222, juin 2013.

26. Les résultats de ces travaux conduits par l'entreprise *Google* ont été publiés initialement dans J. Ginsberg *et al.*, « Detecting influenza epidemics using search engine query data », *Nature*, Vol. 457, 19 février 2009.

du Massachussetts Institute of Technology (MIT), analyse quotidiennement les prix des biens et services proposés sur internet pour produire un indice d'inflation plus précoce que l'indice officiel ; il a ainsi détecté la chute des prix entraînée par la faillite de Lehman Brothers deux mois avant l'indice officiel. La science de l'exploitation des données collectées sur internet n'en est qu'à ses débuts, comme le montrent les difficultés rencontrées par le service de détection des épidémies de grippe de *Google* depuis 2013[27] ; elle n'en est pas moins prometteuse.

- Le *Big Data* ouvre la voie à de **nouvelles méthodes de recherche scientifique**, fondées sur l'induction à partir de l'observation de corrélations statistiques et non plus la déduction à partir d'hypothèses préalables. Ainsi, de nombreux facteurs environnementaux ou génétiques des maladies pourraient être identifiés à partir de l'analyse aléatoire de grandes bases de données. Les mêmes méthodes permettent de détecter les incidents associés à des médicaments : c'est ainsi qu'une étude conduite par la Caisse nationale de l'assurance maladie des travailleurs salariés (CNAMTS), sur la base du répertoire des actes de soins prodigués à chaque assuré social[28], a pu confirmer les troubles cardiaques causés par la consommation du Mediator, mais ceux-ci auraient pu être détectés bien plus tôt si de telles analyses avaient été conduites en continu. Le domaine de la santé n'est pas seul concerné : ainsi, les progrès récents de l'astronomie, par exemple la découverte d'exoplanètes (des planètes extérieures au système solaire), s'expliquent notamment par la capacité à exploiter les volumes de données de plus en plus importants collectés par les télescopes.

- **Le fonctionnement de nombreux services publics pourrait être amélioré**. Dans le domaine de l'énergie, la mise en place de « *réseaux intelligents* » (« *smart grids* »), s'appuyant sur les informations collectées par des compteurs communicants, devrait permettre des économies d'énergie significatives et ainsi réduire les émissions de gaz à effet de serre. Le déploiement des forces de sécurité peut être rendu plus pertinent par l'analyse systématique des données relatives à la criminalité, notamment les lieux et heures des actes de délinquance. La lutte contre la fraude fiscale ou sociale est stimulée par l'identification de types de déclarations associés à une probabilité élevée de fraude.

- Les entreprises exploitent les possibilités du *Big Data* pour **optimiser leurs processus de production**, par exemple dans le domaine de la logistique, ou pour analyser de manière systématique les comportements de leurs clients.

---

27. Si au cours de ses premières années de lancement, le service « *Google Flu Trends* » a mesuré avec exactitude les épidémies de grippe, il les a largement surestimées au cours des hivers 2013 et 2014. Plusieurs hypothèses ont été avancées pour expliquer cette rupture : les requêtes formulées par les internautes auraient été influencées par une couverture médiatique plus importante que de coutume ; l'introduction de l'algorithme de suggestion de mots-clés « *Google Suggest* » aurait faussé le résultat. Cet épisode illustre la sensibilité à des éléments de contexte de ce type d'analyse fondé sur l'observation des comportements. Cf. D. Lazer et al., "The Parable of Google Flu: Traps in Big Data Analysis", *Science*, vol. 343, 14 mars 2014.

28. Il s'agit du Système national d'information inter-régimes de l'assurance-maladie (SNIIRAM) ; cf. l'annexe 3 sur le numérique et la santé pour de plus amples développements.

- Le *Big Data* peut enfin remplir une fonction **d'aide à la décision,** grâce à l'exploitation de toutes les données disponibles par des programmes dotés d'une **intelligence artificielle**. Des programmes informatiques sont par exemple capables de proposer un diagnostic médical en combinant les symptômes et signes cliniques décrits par le médecin et l'analyse systématique de la littérature scientifique.

De nouvelles formes d'interactions entre machines et êtres humains : de l'internet des objets à l'intelligence artificielle

Internet a été conçu pour mettre en relation des machines exploitées par des utilisateurs humains. Des objets fonctionnant de manière autonome sont désormais appelés à y prendre une part croissante, au point qu'on parle « d'internet des objets ». Au vu des progrès rapides de l'intelligence artificielle, les questions posées par l'interaction entre les êtres humains et des machines douées d'une autonomie croissante pourraient prendre une grande place dans les années et les décennies à venir.

En 2013, 61,5 % du trafic internet a été le fait de robots (le terme de robot étant ici utilisé dans un sens général, pour désigner un programme procédant à des connexions sur internet de manière automatisée), le trafic d'origine humaine n'étant que de 38,5 %[29]. La part du trafic humain est en déclin rapide puisqu'elle était encore de 49 % en 2012. Au sein du trafic robotisé, la moitié est le fait d'agents qualifiés de « *bienveillants* », tels que les moteurs de recherche ; l'autre moitié émane d'agents « *malveillants* » (*spams*, qui sont cependant en diminution très rapide ; collecte automatisée de contenus à des fins de reproduction illicite ou de vol de données ; sabotage par des virus ou des attaques par « *déni de service distribué* »[30] ; etc.).

La distinction faite par cette étude entre trafic humain et trafic robotique peut être discutée ; en effet, une grande part du trafic imputé aux robots, notamment celui des moteurs de recherche, est en fait issu de requêtes formulées par des utilisateurs humains. En revanche, l'essor des objets connectés ouvre la perspective de communications véritablement automatisées, non déclenchées par des interventions humaines. L'émergence de « l'internet des objets » est rendue possible par la convergence de trois évolutions technologiques : la capacité à donner à un objet un identifiant unique reconnaissable à distance par d'autres objets[31], et ainsi de lui attribuer une adresse internet[32] ; l'effondrement du prix et de la taille des capteurs pouvant transmettre en temps réel une multitude de

29. Incapsula, *Bot Traffic 2013*.

30. Les attaques par « refus de service distribué » ou « refus de service décentralisé » (traduction de l'anglais « *distributed denial of service* » ou DDoS) consistent à submerger un serveur de requêtes automatiquement générées par un réseau de machines, dans le but d'en faire cesser le fonctionnement.

31. Notamment par l'apposition d'une puce RFID (*Radio Frequency Identification*) ; il s'agit, selon la présentation donnée par la CNIL, « *d'une puce informatique couplée à une antenne lui permettant d'être activée à distance par un lecteur et de communiquer avec ce dernier* ».

32. La norme actuelle de définition des adresses IP, le protocole « IPv4 », permet d'attribuer 2^{32} adresses différentes, soit environ 4,3 milliards d'adresses. Cet espace arrive aujourd'hui à saturation et c'est pourquoi une transition vers le protocole « IPv6 », où l'espace est de

données (température, humidité, localisation, vitesse, tension artérielle, etc.) ; le développement de réseaux de communication sans contact en mesure de transmettre ces données. Comme pour le *Big Data*, les applications existantes ou envisagées pour les objets connectés sont multiples et en constant développement. L'on ne mentionnera ici que quelques illustrations dans les domaines suivants :

- **Activités de loisir** : sont déjà développées et en voie de commercialisation, à la date de cette étude, la mesure de la performance (et le cas échéant, le partage de celle-ci sur les réseaux sociaux), lors d'un exercice physique par des capteurs de vitesse ou de rythme cardiaque ; la lecture de messages ou l'écoute de musique au moyen de montres ou de bracelets connectés ; l'utilisation d'une caméra ou d'un micro accompagné de l'accès à de nombreux services de la plateforme *Google* sur les lunettes connectées développées par cette entreprise (« *Google Glass* »).

- **Santé** : de nombreux dispositifs ont été mis sur le marché au cours des dernières années, suscitant la naissance de l'expression de « m-santé » (« m » pour mobilité). Ils remplissent d'ores et déjà une gamme de fonctions allant de la prévention, par l'incitation à l'exercice physique ou à une alimentation équilibrée, au suivi des malades chroniques, par exemple en aidant les personnes diabétiques à maîtriser leur glycémie. Le suivi en continu de certaines données biologiques pourrait aussi permettre de déceler de manière précoce des accidents graves tels que des infarctus, permettant un gain important en termes de chances de survie et de limitation des séquelles.

- **Logement** : à l'intérieur du domicile, le déploiement de « compteurs intelligents » ou de thermostats connectés vise la réalisation d'économies d'énergie et une adaptation plus fine aux besoins des occupants. À moyen terme, c'est la perspective d'une « *maison connectée* » qui pourrait se dessiner, offrant aux particuliers la possibilité de programmer, à partir d'un unique système d'exploitation, l'ensemble de leurs appareils domestiques, leur consommation d'électricité et d'énergie ou encore la sécurité de leur logement.

- **Transports** : la « voiture connectée » pourrait être équipée de capteurs détectant l'usure de ses composants, d'objets communiquant avec les autres véhicules pour renforcer la sécurité et d'une interface permettant d'accéder aux mêmes contenus (musique, géolocalisation, etc.) que ceux accessibles depuis un smartphone ou une tablette. Elle pourrait même être une voiture sans chauffeur, de tels véhicules étant déjà expérimentés, notamment en Californie et à Lyon.

L'internet des objets apparaît ainsi en mesure de rendre de nombreux services aux particuliers et de permettre l'éclosion de nouveaux marchés. Son essor va sans doute changer la nature d'internet. D'une part, alors qu'internet a surtout servi jusqu'ici à la transmission de contenus immatériels (informations, musique, images, etc.), le développement des objets connectés le fait entrer dans l'univers matériel, démultipliant ainsi sa capacité à transformer des pans entiers de notre vie quotidienne. D'autre part, ce développement redéfinit les places respectives

---

2^{128} adresses, est actuellement en cours. La transition vers IPv6 doit notamment permettre l'attribution des dizaines de milliards d'adresses que pourraient nécessiter les objets connectés.

des êtres humains et des machines dans le fonctionnement d'internet, avec l'idée sous-jacente que les machines sont à certains égards plus aptes que les humains à produire des données pertinentes. Kevin Ashton, un des inventeurs des puces RFID, qui revendique la paternité de l'expression « *internet des objets* », présente ainsi cette problématique : « *Le problème est que les individus ont un temps, une attention et une précision limités – ce qui implique qu'ils ne sont pas très bons pour transmettre des données sur le monde réel. (…) Les idées et l'information sont importantes, mais les choses le sont plus encore. (…) Si nous avions des ordinateurs qui savent tout ce qu'il y a à savoir sur les choses – en utilisant des données collectées sans notre intervention – nous serions capables de tout suivre et de tout mesurer, et de réduire considérablement les déchets, les pertes et les coûts. Les puces RFID et les capteurs permettent aux ordinateurs d'observer, d'identifier et de comprendre le monde – sans les limites des données fournies par les êtres humains.* »[33].

La plupart des objets connectés présentés ci-dessus sont des objets inintelligents limités par leur conception à la captation et à la retransmission d'un nombre limité de données. Les progrès de l'intelligence artificielle laissent cependant entrevoir la perspective d'une nouvelle génération d'objets plus autonomes, capables d'apprendre et de se comporter d'une manière non entièrement définie par leur programmation. Dans son étude prospective, le CGSP envisage l'avènement de ces objets intelligents, qu'il qualifie de robots, à partir de 2020. Dès aujourd'hui, l'assistant vocal *Siri,* conçu par *Apple*, est capable de comprendre les instructions formulées par son utilisateur et de lui répondre en « *langage naturel* ». Le thermostat connecté *Nest* est capable d'un apprentissage automatique (désigné en anglais par l'expression « *machine learning* ») d'après les habitudes de son utilisateur. Le gouvernement américain a lancé en 2013 un programme de recherche doté de 100 millions de dollars pour simuler, à l'horizon d'une décennie, le fonctionnement du cerveau humain.

Des réflexions sur l'interaction entre l'homme et des machines intelligentes ou sur la manière dont le rapport à la machine transforme les êtres humains, qui pouvaient sembler relever de la science-fiction il y a encore quelques années, acquièrent ainsi progressivement une certaine actualité. Les questions portent aussi bien sur l'efficacité technique, scientifique et économique que sur les enjeux éthiques et juridiques. Sur le plan de l'efficacité, la combinaison des capacités intuitives du cerveau humain et des capacités de calcul des machines pourrait par exemple permettre de résoudre des problèmes scientifiques encore sans solution[34].

---

33. K. Ashton, « That 'Internet of Things' Thing », *RFID Journal*, juin 2009. Traduction des auteurs.

34. Des chercheurs sont parvenus à surmonter des problèmes de prédiction de la structure tridimensionnelle des protéines (problème dit du « repliement des protéines »), que la puissance de calcul des ordinateurs seule ne permettait pas de résoudre, en sollicitant l'intervention d'êtres humains à travers un jeu vidéo dénommé *« Foldit »* (en français « plie-la ») ; cette découverte pourrait donner lieu à des applications dans la lutte contre le sida. Cf. F. Khatib *et al.*, « Crystal structure of a monomeric retroviral protease solved by protein folding game players », *Natural Structural & Molecular Biology*, 18, 1175-1177 (2011).

Les questions éthiques et juridiques portent sur la manière d'appréhender la responsabilité des robots intelligents, la nécessité d'imposer des limites à leurs capacités d'action ou la licéité d'une amélioration des capacités humaines par le recours à l'intelligence artificielle. Le courant dit « *transhumaniste* » revendique le droit à l'amélioration des capacités physiques et mentales des êtres humains, comme une liberté fondamentale ; l'entreprise *Google*, qui investit dans le domaine de la robotique et de l'intelligence artificielle, a recruté l'un des principaux chefs de file de ce courant, Raymond Kurzweil, comme directeur de l'ingénierie, et son PDG Eric Schmidt évoque la perspective d'une « *humanité augmentée* »[35]. Pourtant, comme en matière de bioéthique, il ne suffit pas qu'une possibilité soit ouverte par la technique pour qu'il soit légitime de la mettre en œuvre, et l'on peut penser qu'une éthique de l'interaction entre les êtres humains et les machines intelligentes, définissant les limites de ce qui doit être admis, reste largement à bâtir.

1.1.2. Des révolutions économiques : la valorisation par la donnée

La transformation d'un nombre croissant de secteurs d'activité

La question du poids du numérique dans l'économie n'appelle pas une réponse univoque. Une première approche, étroite, consiste à délimiter le secteur de l'économie numérique et à mesurer la part du produit intérieur brut (PIB) qu'il représente. Plusieurs travaux convergent sur la définition de ce « *cœur de l'économie numérique* », selon la formule d'un rapport de l'Inspection générale des finances (IGF)[36]. Il comporte le secteur des télécommunications, la production d'équipements informatiques, les services numériques (édition de logiciels, sociétés de services et d'ingénierie informatique (les SS2I), etc.) et les activités économiques réalisées sur internet (e-commerce, musique, vidéo à la demande et jeux en ligne, etc.)[37].

Le poids de cette économie numérique *stricto sensu* apparaît significatif mais ne doit pas être surestimé : sur un échantillon de 13 pays analysés par le cabinet McKinsey, elle représente en moyenne 3,4 % du PIB, ce qui est certes supérieur sur l'échantillon à l'éducation ou à l'agriculture mais près de deux fois inférieur aux services financiers. La proportion serait de 2,6 % en Chine, de 3,1 % en France, de 3,2 % en Allemagne et en Inde, de 3,8 % aux États-Unis, de 4 % au Japon, de 4,6 % en Corée du sud et de 5,4 % au Royaume-Uni. Selon le rapport de l'IGF, qui ne concerne que la France et retient une autre méthodologie, le cœur de l'économie numérique représente 5,2 % du PIB (cf. graphique ci-dessous). En outre, contrairement à une idée reçue, le poids de l'économie numérique apparaît relativement stable : selon l'IGF, il n'a pas évolué en France depuis dix ans. Le CGSP explique cette stabilité, également observée dans d'autres pays, par la chute

35. Notamment dans son ouvrage *The New Digital Age*, *Reshaping the Future of People, Nations and Business,* Knopf, 2013.

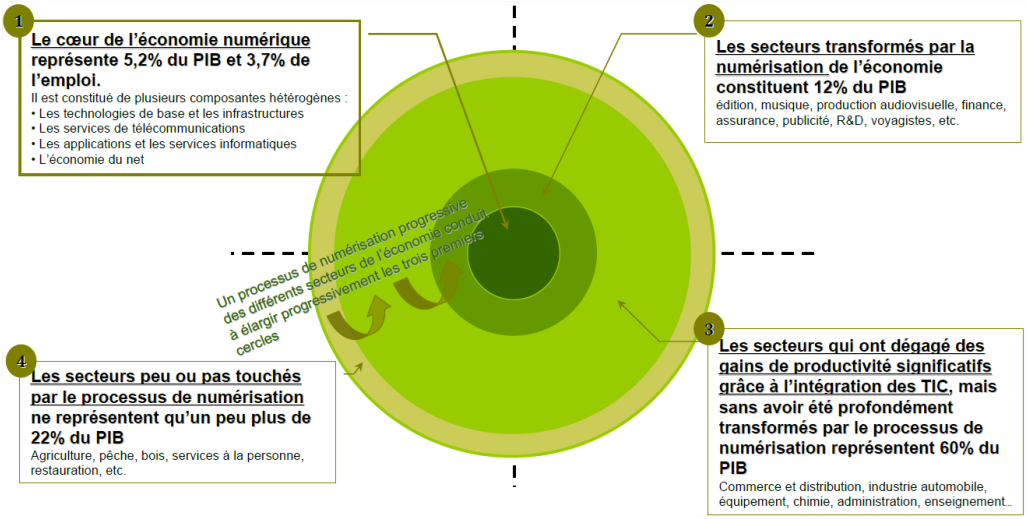
36. IGF, *Le soutien à l'économie numérique et à l'innovation*, janvier 2012.

37. Outre le rapport précité de l'IGF, d'autres rapports parviennent à une définition voisine : OCDE, "Measuring the Internet Economy: A Contribution to the Research Agenda", *OECD Digital Economy Papers*, n° 226, OECD Publishing, 2013 ; McKinsey Global Institute, *Internet matters : The Net's sweeping impact on growth, jobs, and prosperity*, mai 2011.

constante des prix dans ce secteur, qui annulerait la croissance des volumes : ainsi, entre 1980 et 2010, l'indice des prix du secteur des télécommunications a reculé de 40 %, alors que l'indice des prix global progressait de 50 %.

Cependant, une autre approche est possible car le numérique fait ressentir ses effets bien au-delà des quelques secteurs précédemment identifiés. Internet et les technologies numériques sont souvent qualifiés de « *technologies génériques* » par les économistes (traduction de l'anglais « *general purpose technologies* »), c'est-à-dire qu'ils peuvent être utilisés par l'ensemble des secteurs d'activité et en accroître la productivité. Les technologies génériques se reconnaissent à trois caractéristiques[38] : leur ubiquité, c'est-à-dire leur utilisation potentielle par tous les secteurs d'activité ; leur capacité à y stimuler l'innovation ; la diminution rapide de leur coût[39]. Dans le passé, la machine à vapeur et l'électricité ont été les technologies génériques à l'origine des première et deuxième révolutions industrielles.

Évaluation du poids de l'économie numérique en France et de l'intensité de l'usage du numérique par les autres acteurs



Source : Inspection générale des finances, Le soutien à l'économie numérique et à l'innovation, rapport n° 2011-M-060-02, janvier 2012, p. 21.

Certains secteurs, ceux du « *2e cercle* » de la typologie de l'IGF, ont d'ores et déjà connu une transformation profonde, même si elle reste inachevée, de leur organisation et de leur modèle économique en raison de l'irruption des technologies numériques. C'est par exemple le cas de la presse écrite (a) et de l'industrie des biens culturels (b).

38. Bresnahan, T. F. *and* M. Trajtenberg, "General purpose technologies 'Engines of growth'?", *Journal of Econometrics* 65 (1), 83106, 1995.

39. En utilisant un indice de recours aux technologies de l'information et de la communication (TIC) construit par l'INSEE, l'IGF a établi une typologie des secteurs d'activité sous forme de cercles concentriques, du cœur de l'économie numérique aux secteurs, aujourd'hui minoritaires, où l'utilisation de ces technologies est marginale.

(a) La presse écrite a vu ses recettes ainsi que ses modes de production et de diffusion fortement remis en cause par l'essor du numérique. Les deux sources de revenus de la presse écrite, les ventes et la publicité, ont été affectées : les ventes en raison des habitudes de gratuité associées à l'utilisation d'internet, d'autant plus que de nombreux organes de presse ont fait le choix dans un premier temps de rendre la plupart de leurs contenus accessibles gratuitement en ligne ; la publicité du fait de la plus grande attractivité d'internet pour les annonceurs, celui-ci permettant de mesurer finement la performance d'une campagne et de proposer des annonces personnalisées et contextualisées. Les modes de production et de diffusion ont été bouleversés par l'actualisation en continu que permet internet, par la très forte percée depuis quelques années des terminaux mobiles (smartphones et tablettes) comme supports de lecture, par le développement de l'interaction avec les lecteurs (commentaires en réaction aux articles, hébergements de forums et de blogs sur les sites de presse, etc.) et, enfin, par le développement de nouvelles portes d'accès aux contenus de presse (moteurs de recherche, qui constituent en outre des services dédiés à l'agrégation des contenus de presse, réseaux sociaux, etc.). Une controverse s'est développée en France entre la presse et l'entreprise *Google*, en raison de la reproduction des contenus des titres de presse par le service *Google Actualités* : les organes de presse revendiquaient le paiement par *Google* de droits de reproduction, tandis que cette entreprise arguait de son rôle d'apporteur de lectorat ; un accord a été signé en février 2013 sous les auspices de l'État, prévoyant la mise en place d'un fonds de 60 millions d'euros financé par *Google* pour soutenir le développement de la presse dans le numérique. Ce type de controverses n'est pas limité à la France puisque le patron d'Axel Springer, premier groupe de presse allemand, a écrit en avril 2014 une lettre ouverte au patron de cette entreprise américaine, expliquant qu'il avait « *peur de Google* », en raison de la dépendance économique de la presse à son égard[40]. Les entreprises de presse sont nombreuses au sein de la coalition « *Open Internet Project* », qui a saisi la Commission européenne en mai 2014 d'une plainte contre *Google* pour abus de position dominante (cf. *infra* 1.3.2).

À ce stade, malgré ses efforts de développement en ligne, la presse écrite française, n'a pas avoir stabilisé son modèle économique : les ventes annuelles, stables jusqu'en 2007, ont chuté de 7 milliards à 5 milliards de numéros entre cette date et 2011 ; la perte totale de chiffre d'affaires entre 2000 et 2010 atteint 925 millions d'euros, soit près de 10 %, et les revenus tirés de la presse en ligne sont loin d'avoir pris le relais puisqu'ils ne représentent encore que 3,3 % du chiffre d'affaires[41].

(b) Le bouleversement connu par le secteur des biens culturels musicaux et audiovisuels est encore plus profond. Par sa puissance de reproduction, de diffusion et de référencement, le numérique permet un élargissement démesuré de l'accès aux œuvres culturelles, si bien que la période antérieure, où cet accès

40. « Le patron d'Axel Springer : "Nous avons peur de Google" », *Le journal du Net*, 22 avril 2014.

41. Chiffres extraits de D. Assouline, *Rapport fait au nom de la commission de la culture, de l'éducation et de la communication du Sénat sur la proposition de loi tendant à harmoniser les taux de la taxe sur la valeur ajoutée applicables à la presse imprimée et à la presse en ligne*, février 2014.

dépendait de l'acquisition de supports physiques, apparaît rétrospectivement comme une ère de rareté. Le développement du numérique a d'ailleurs été nourri par le désir d'accès aux œuvres culturelles, qui a constitué l'une des principales motivations des ménages pour s'équiper en terminaux et en abonnements à internet. Les industries de production et de distribution de ces biens culturels ont subi un double choc, celui de l'offre illicite et celui du déplacement du partage de la valeur. Les pratiques de consommation méconnaissant les droits de propriété intellectuelle, reposant sur le téléchargement de pair à pair, le téléchargement direct ou la diffusion en flux (le *streaming*) se sont développées de manière massive, dès le début des années 2000 pour la musique, plus tardivement pour la vidéo en raison des volumes plus importants des fichiers. Elles ont créé une habitude de gratuité, en particulier chez les jeunes générations, et un recul corrélatif du « *consentement à payer* » pour l'accès aux contenus, selon la formule d'un rapport de Pierre Lescure[42]. Par ailleurs, si des services numériques légaux d'accès aux œuvres culturelles se sont également développés, les acteurs installés de l'industrie des biens culturels n'y ont pris qu'une petite part. Un déplacement de la valeur s'est produit au profit des nouveaux acteurs de l'économie numérique, dits « *over the top* » : certains ont su proposer une offre licite plus attractive (le service *iTunes* d'*Apple* et les sites de diffusion *Deezer* et *Spotify* captent à eux trois 90 % du marché de la musique en ligne), d'autres bénéficient simultanément des pratiques de consommation licite et illicite (vendeurs de terminaux, plateformes de partage des contenus telles que *Youtube* et *Dailymotion*). Ces évolutions affectent à la fois la rentabilité de certaines industries et la rémunération des créateurs, dont les modalités doivent être redéfinies pour s'adapter aux nouvelles pratiques licites, ainsi que les mécanismes de soutien à la création et à la diversité culturelle mis en place avant le développement des usages numériques (cf. *infra* 1.3.3).

La transformation de ces deux secteurs est manifeste et connue du grand public, qui en fait l'expérience dans ses usages quotidiens. Sa précocité peut s'expliquer par la dématérialisation complète qu'a permis le numérique dans ces activités.

Plus récente et sans doute moins bien perçue à ce jour est la transformation d'un nombre croissant de secteurs non dématérialisés. Ainsi :

- **L'hôtellerie** fait face à une double évolution. D'une part, une proportion croissante de ses clients réservent leurs chambres par l'intermédiaire de plateformes telles que *Booking* ou *Expedia*. Le référencement par ces plateformes devient un enjeu crucial et les hôteliers acquittent à cette fin des commissions importantes qui réduisent leurs marges bénéficiaires ; comme dans le secteur des biens culturels, les services mis en place par les acteurs installés n'ont pas acquis à ce jour une audience comparable à celle de ces nouveaux acteurs. D'autre part, des services de partage de pair à pair se développent, qui permettent à des particuliers de proposer leur logement pour héberger des touristes, certains sur un modèle payant (*Airbnb*), d'autre sur un modèle gratuit (*Couchsurfing*).

42. P. Lescure, *Culture – acte 2. Contribution aux politiques culturelles à l'ère numérique*, mai 2013.

- Second employeur du pays après l'État, ***La Poste*** connaît deux tendances opposées liées au numérique : un déclin inéluctable du courrier, qui s'accélère depuis 2008 (de l'ordre de 1 % par an entre 2001 et 2007, la chute est aujourd'hui de 6 % à 9 % par an[43]) en raison de l'adoption par les particuliers, les entreprises et les administrations des échanges électroniques ; un développement de l'activité colis lié à la progression du commerce en ligne.

- **Le commerce et la grande distribution** voient comme l'hôtellerie se développer le rôle des « places de marché » sur internet, telles que *Amazon* ou *e-Bay*, qui s'interposent de plus en plus souvent entre les vendeurs et leurs clients. Les progrès des sites comparateurs, voire des méta-comparateurs (les sites qui agrègent les résultats de plusieurs comparateurs), stimulent la concurrence par les prix et permettent aux consommateurs de procéder à des choix plus avertis sur les produits techniques. L'analyse numérisée du panier de produits achetés par le consommateur, assortie d'une invitation à souscrire des avantages de fidélisation, permet de cibler les habitudes d'achat. Les progrès très rapides des « *drives* », ces points de retrait des articles commandés sur internet, ont suscité l'intervention du législateur qui leur a étendu le régime d'autorisation de l'urbanisme commercial dans le cadre de la loi pour l'accès au logement et un urbanisme rénové du 24 mars 2014.

- Le numérique a renouvelé la problématique ancienne de l'ouverture à la concurrence des **taxis**. La réservation par internet, notamment au moyen d'un smartphone, et la géolocalisation, ont rendu plus attractif le service proposé par les véhicules de tourisme avec chauffeur (VTC), qui se distinguent des taxis par l'exigence de réservation préalable et l'interdiction de stationner et de circuler sur la voie publique dans le but de chercher des clients (la « maraude », dont les taxis ont le monopole légal). Des sociétés telles qu'*Uber* ou *LeCab*, dont l'objet est de fournir une plateforme de réservation de VTC accessible par voie numérique, se sont développées en quelques années. La concurrence accrue, permise par l'essor du numérique, entre une profession dont l'exercice est subordonné à l'octroi d'une licence et une autre profession libéralisée par la loi du 22 juillet 2009 de développement et de modernisation des services touristiques, suscite d'importantes controverses. Après que le juge des référés du Conseil d'État a suspendu un décret imposant aux VTC un délai de réservation préalable de quinze minutes[44], une mission de concertation, dont les préconisations sont reprises par une proposition de loi, a recommandé de maintenir le monopole de la maraude des taxis en le modernisant ; une « *maraude électronique* » serait créée, consistant en une géolocalisation des taxis, permettant aux consommateurs de réserver par leur smartphone le taxi le plus proche[45].

---

43. Cf. Cour des comptes, *La Poste : un service public face à un défi sans précédent, une mutation nécessaire*, rapport public thématique, juillet 2010 ; « L'avenir de La Poste après le courrier », *Le Monde*, 23 septembre 2013.

44. JRCE, 5 février 2014, *SAS Allocab, Société Voxtur et autres*, n° 374524, inédit.

45. Cf. T. Thévenoud, *Un taxi pour l'avenir. Des emplois pour la France*, Mission de concertation Taxis – VTC, avril 2014 ; proposition de loi relative aux taxis et aux voitures de transport avec chauffeur, n° 2046, déposée le 18 juin 2014 à l'Assemblée nationale.

- **Les processus industriels** sont transformés par le numérique. Les imprimantes 3D abaissent considérablement le coût de production des prototypes ou des objets personnalisés, comme les prothèses dans le domaine des dispositifs médicaux ; elle pourrait faciliter l'adaptation réactive de la production aux besoins. Les capacités des robots d'interagir de manière plus autonome avec leur environnement sont démultipliées par le numérique. Les capteurs connectés peuvent rendre la maintenance des équipements industriels beaucoup plus efficace, par une connaissance fine de l'état d'usure des pièces et des matériels.

Des modèles d'affaires spécifiques

Dans tous ces secteurs, le numérique manifeste sa capacité à bouleverser les règles du jeu et les positions établies, son caractère « disruptif » selon la formule souvent employée par les analystes du phénomène. Les modèles d'affaires des entreprises du numérique présentent des caractéristiques spécifiques[46].

- **Des modèles tournés vers la croissance :** les entreprises du numérique privilégient la croissance sur la profitabilité à court terme. Selon la formule employée par l'une des personnalités auditionnées, leurs dirigeants « *se comportent davantage comme des généraux d'Empire que comme des hommes d'affaires* ». L'entreprise *Amazon* a ainsi perdu 3 milliards de dollars entre sa création en 1995 et 2003, date de ses premiers bénéfices ; encore en 2013, ses bénéfices, de 274 millions de dollars, demeurent limités au regard de sa capitalisation boursière (164 milliards de dollars en février 2014). Certaines entreprises acceptent même de ne réaliser qu'un chiffre d'affaires limité durant plusieurs années pour faire croître leur clientèle. *Facebook* a attendu plusieurs années avant de diffuser des publicités à ses utilisateurs. L'application de messagerie instantanée *Whatsapp* a acquis 400 millions d'utilisateurs en quelques années sans diffuser de publicité, en proposant des services gratuits la première année puis au prix de 0,99 cents par an. Ces stratégies de croissance peuvent s'expliquer notamment par l'importance des effets de réseau : selon la loi dite *de Metcalfe*, (du nom du concepteur du protocole *Ethernet* dans les années 1970), l'utilité retirée de l'appartenance à un réseau est proportionnelle au carré du nombre des utilisateurs de celui-ci ; il est donc capital pour ces entreprises de faire croître rapidement leur nombre d'utilisateurs. Le financement des phases de croissance est assuré par le recours au capital-risque ; les investisseurs, qui acceptent de financer des projets dont la probabilité de réussite est faible et incertaine, sont rémunérés par les plus-values très importantes générées en cas de succès.

- **Des stratégies de redéfinition des frontières des marchés :** Les entreprises du numérique tendent à redéfinir les frontières des marchés où elles exercent leur activité, dans leur phase de croissance comme dans leur phase de maturité. Ce

46. Ces caractéristiques ont été mises en évidence notamment par : N. Colin et H. Verdier, *L'âge de la multitude. Entreprendre et gouverner après la révolution numérique*, Armand Colin, 2012 ; P. Collin et N. Colin, *Mission d'expertise sur la fiscalité de l'économie numérique*, rapport au ministre de l'économie et des finances, au ministre du redressement productif, au ministre délégué chargé du budget et à la ministre déléguée chargée des petites et moyennes entreprises, de l'innovation et de l'économie numérique, janvier 2013 ; P. Bellanger, *La souveraineté numérique*, Stock, 2014.

phénomène n'est pas propre à l'économie numérique, mais il y est plus marqué, en raison de la rapidité des cycles d'innovation. Dans leur phase de croissance, les entreprises du numérique sont souvent porteuses d'une innovation qui fait surgir un nouveau marché ou modifie le périmètre de marchés existants. Ainsi, les réseaux sociaux apparus dans la première moitié des années 2000 constituaient alors un service tout à fait nouveau ; les services de cartographie en ligne (*Mappy*, *Google Maps*, *Open Street Map*, etc.) ont profondément modifié le périmètre du marché de la cartographie. Arrivées à maturité, ces mêmes entreprises ne se satisfont pas pour autant du domaine qu'elles ont constitué et cherchent en permanence à en redéfinir les frontières. À partir de l'activité de moteur de recherche, *Google* veut devenir un service de recommandation d'hôtel (*Google Hostel*) ou de recherche académique (*Google Scholar*). Les activités des entreprises du numérique tendent à s'interpénétrer. Etroitement entendu, le marché des moteurs de recherche est celui occupé par *Bing*, *Google* et *Yahoo!* ; cependant, *Amazon* et *Facebook* peuvent aussi être utilisés comme des moteurs de recherche. L'instabilité des frontières des marchés est une source de difficulté pour la régulation de la concurrence ou la mise en œuvre de réglementations sectorielles (cf. *infra* 1.3.2).

- **Des stratégies de plateforme** : dans les exemples sectoriels cités ci-dessus, le bouleversement vient souvent de l'irruption d'un acteur qui prend une place privilégiée de porte d'accès aux consommateurs. Celui-ci devient ainsi une plateforme incontournable pour exercer son activité, et en retire bien sûr de la valeur. Une manière d'approfondir cette stratégie de plateforme est d'ouvrir délibérément ses ressources à d'autres acteurs. L'une des clés du succès d'*Apple* a été de permettre à une multitude de sociétés de proposer des applications sur ses terminaux *iPhone* et *iPad* ; les commissions versées par ces sociétés représentent aujourd'hui une part considérable de ses revenus. De même, *Amazon* est devenue un acteur majeur de l'informatique en nuage en proposant à des tiers les ressources informatiques qu'elle avait constituées pour exercer son activité de distributeur. La mise à disposition d'une plateforme se fait au moyen d'une interface de programmation d'applications (« *application programming interface* » ou API), facilitant le développement de services par des tiers. La relation de plateforme à application est mutuellement profitable. Elle est toutefois à l'avantage de la plateforme : l'application a davantage besoin de la plateforme que l'inverse. Il en résulte une asymétrie qui pose là encore des difficultés à la régulation concurrentielle (cf. *infra* 1.3.4).

- **Une valorisation intensive des données** : Les entreprises du numérique ont démontré leur capacité à tirer de l'utilisation des données, dont les possibilités ont été présentées ci-dessus (cf. 1.1.1), une source de revenus majeure et en forte croissance. La publicité est un premier mode de valorisation des données. Le fait de cibler une campagne de publicité en fonction des caractéristiques de ses spectateurs probables – par exemple en diffusant des publicités pour des jouets à l'heure des programmes télévisés pour enfants – n'est pas une nouveauté. Le numérique démultiplie cependant les possibilités de ciblage. Trois techniques se sont notamment développées : la publicité contextuelle, la publicité personnalisée et la publicité comportementale

Les différentes formes de publicité ciblée

La **publicité contextuelle** consiste à proposer des publicités définies en fonction du contenu des pages visitées sur internet ou d'une requête formulée sur un moteur de recherche. Il s'agit de la première activité développée par *Google* : son service *AdWords* permet à des annonceurs d'acheter des mots-clés pour que leurs publicités soient affichées lorsqu'un utilisateur cherche l'un de ces mots-clés ; quant à son service *AdSense*, il permet à des sites tiers d'afficher des publicités au contenu en rapport avec la page visitée.

La **publicité personnalisée** part directement des caractéristiques de l'individu, connues du site visité. Cette technique peut notamment être utilisée par les sites dont l'utilisation implique l'ouverture d'un compte personnel, comme *Facebook* et depuis quelques années *Google*. Lors de l'inscription, le site recueille un certain nombre d'informations sur la personne (sexe, âge, adresse), pertinentes pour le ciblage publicitaire. Une discothèque de Limoges peut ainsi acheter auprès de *Facebook* un espace publicitaire sur les comptes de toutes les personnes de 18 à 25 ans habitant dans Limoges et ses environs.

La **publicité comportementale** se fonde non sur les caractéristiques de la personne mais sur l'observation de son comportement en ligne. Le « reciblage » est une forme de publicité comportementale : il consiste à envoyer des publicités à un internaute qui soient en rapport non avec le site qu'il est en train de visiter, mais avec un produit pour lequel il a manifesté son intérêt en visitant dans un passé proche un autre site. Il est par exemple mis en œuvre par la société française *Criteo*. De manière plus élaborée, le ciblage comportemental peut se fonder sur tout un historique de navigation, dont il est possible de déduire des centres d'intérêt ou une intention d'achat. Cet historique peut être accessible par diverses sources :

- le navigateur utilisé par l'internaute peut livrer l'historique des sites visités ;

- les entreprises qui proposent des services de régie publicitaire pour des sites tiers sont en mesure de reconnaître un internaute d'un site à l'autre (notamment par l'enregistrement de *cookies* sur son terminal) et d'accumuler ainsi des informations à son sujet ;

- les fournisseurs d'accès à internet (FAI) sont techniquement en mesure de disposer d'un historique complet de la navigation de leurs abonnés ; en 2011-2012, *Orange* a expérimenté un tel service, dénommé *Orange Préférences*, permettant aux abonnés qui le souhaitaient de recevoir des publicités ciblées sur la base de leur navigation, mais l'expérimentation n'a pas été poursuivie.

Ces différentes formes de ciblage peuvent se combiner. Ainsi, les boutons « j'aime » de *Facebook* et « + 1 » de *Google*, présents sur de nombreux sites tiers, permettent à ces sociétés de compléter les données dont elles disposent sur les personnes utilisant leurs services par des données sur la navigation de ces personnes.

La publicité ciblée joue un rôle déterminant dans les modèles d'affaires de nombreuses entreprises du numérique. Elle est la principale source de revenus de *Google* et de *Facebook*. Elle permet à de nombreux acteurs de proposer sur internet des services gratuits en tout ou partie, par exemple en matière de presse ou de musique en ligne. C'est elle qui finance ce qu'on peut qualifier de culture de la gratuité sur internet, qui demeure prédominante. Les économistes qualifient ces modèles de « *modèles bifaces* », car ces entreprises travaillent en réalité pour deux catégories de clients : les internautes, qui ont accès à la face gratuite du service ; les annonceurs, qui ont accès à la face payante.

L'ampleur de la publicité ciblée peut cependant faire oublier que les données sont aussi, et peut-être surtout, utilisées pour améliorer le service lui-même. En s'appuyant sur une typologie proposée par le rapport de Pierre Collin et Nicolas Colin sur la fiscalité du numérique[47], on peut distinguer les utilisations suivantes des données :

- **Le pilotage de la performance du service** : le numérique permet de disposer de données très fines et collectées en temps réel sur la performance d'un service, notamment sur la satisfaction des utilisateurs. Il est ainsi possible de savoir très vite si la mise à jour d'une application est appréciée et, si ce n'est pas le cas, de la retirer.

- **La personnalisation du service** : la collecte de données personnelles ouvre de multiples possibilités de différencier le service selon les utilisateurs. Pour une même requête, *Google* renvoie des résultats différents selon les utilisateurs, car son algorithme prend en compte les centres d'intérêt de ceux-ci, révélés par leurs requêtes précédentes.

- **L'agrégation des préférences individuelles pour produire des services plus performants** : le modèle de nombreux sites repose sur l'exploitation statistique des préférences révélées par les internautes. Le moteur de recherche de *Google* classe les sites internet par ordre de pertinence en fonction du nombre de liens hypertexte renvoyant vers chacun d'entre eux. Le site de recommandations de voyage *TripAdvisor* repose sur le classement des préconisations faites par ses utilisateurs. *Amazon* exploite les corrélations entre les achats de tous ses clients pour proposer des achats complémentaires, sous la formule « *ceux qui ont acheté le livre A ont aussi aimé les livres B et C et le disque D* ».

- **La fourniture du service** : dans certains cas, la collecte, l'exploitation et la transmission des données font plus que permettre une amélioration du service ; elles sont le service lui-même. C'est notamment le cas des objets connectés, qu'il s'agisse de mesurer la performance lors d'un exercice physique ou d'alerter sur l'état préoccupant d'une personne atteinte de troubles cardiaques.

Enfin, un dernier mode de valorisation des données consiste à les céder ou à les rendre accessibles à des tiers, sans nécessairement en informer les personnes concernées. Dans l'économie numérique d'aujourd'hui, les données ne restent pas chez ceux qui les ont collectées, elles sont en permanence échangées et

47. P. Collin et N. Colin, *op. cit.*, p. 56.

recombinées. Certains acteurs, qualifiés de « *courtiers en données* » (de l'anglais « *data brokers* ») ont même pour raison sociale d'acquérir et de vendre des données personnelles. Il existe un marché des données en pleine expansion ; les questions soulevées par son existence et ses modalités de fonctionnement seront abordées plus loin (cf. *infra* 2.2.1).

Plusieurs travaux se sont efforcés de quantifier la valeur des données et de prévoir son évolution. Selon une étude du *Boston Consulting Group*[48], la valeur des données des Européens était en 2011 de 315 milliards d'euros et pourrait atteindre 1 000 milliards d'euros en 2020. Dans une autre étude portant sur un périmètre différent, puisqu'elle concerne l'ensemble du *Big Data* et pas seulement les données, le cabinet *McKinsey* a estimé que l'utilisation des données pouvaient générer un surplus pour le consommateur de 600 milliards d'euros[49]. S'il n'existe pas encore de consensus sur les méthodes à suivre pour évaluer la valeur économique des données[50], ces travaux convergent pour souligner l'ampleur de leur rôle dans la transformation de l'économie.

1.1.3. Des révolutions de société : à nouvelles interactions, nouvelles normes sociales ?

Les technologies numériques ont été adoptées à une vitesse exceptionnelle, sans précédent dans l'histoire des innovations. Elles ouvrent aux individus des possibilités inédites de collaborations, ce qui favorise la participation des citoyens et la transparence dans l'action des pouvoirs publics. Si ces évolutions sont en règle générale saluées de manière positive, l'impact des usages du numérique sur les normes sociales en matière de vie privée fait en revanche débat.

Une adoption fulgurante des usages du numérique

Une courbe exponentielle commence par croître lentement. Entre 1973, date d'adoption du protocole TCP/IP, et 1995, internet n'avait conquis que 16 millions d'utilisateurs. Mais il n'a ensuite fallu que dix ans pour que le premier milliard soit atteint (en 2005), puis cinq ans pour le deuxième milliard (en 2010). Jamais une innovation technique n'avait connu un rythme d'adoption aussi rapide. Aux États-Unis, il a fallu 50 ans pour que la moitié des Américains se dote d'un téléphone, 20 ans pour que la moitié accède à l'électricité et 15 ans pour que la moitié acquière une automobile ; il n'aura fallu que 10 ans, entre 1990 et 2000, pour que la moitié dispose d'une connexion internet[51]. Une même rapidité peut être observée pour l'adoption de certains services sur internet. *Facebook*, créé en 2004, a atteint 200 millions d'utilisateurs en 2009, puis 1 milliard en 2012. *Whatsapp* n'a mis que cinq ans pour conquérir 500 millions d'utilisateurs.

---

48. Boston Consulting Group, *The Value of Our Digital Identity*, novembre 2012.
49. McKinsey Global Institute, *Big Data : The next frontier for innovation, competition and productivity*, mai 2011.
50. Cf. pour une discussion sur ces méthodes OCDE, « Exploring the Economics of Personal Data », *OECD Digital Economy Papers*, n° 220, OECD Publishing, avril 2013.
51. Chiffres cités par P. Collin et N. Colin, *op. cit*, p. 8.

Dans la période la plus récente, les usages mobiles d'internet, sur smartphone ou sur tablette, ont progressé encore plus qu'internet dans son ensemble. Le nombre d'utilisateurs d'internet mobile pourrait dépasser cette année celui des utilisateurs du fixe. Sur le seul quatrième trimestre 2012, 207 millions de smartphones ont été vendus, soit un chiffre supérieur à la population du Brésil. La croissance des usages mobiles est particulièrement forte dans les pays en développement, où le déploiement des infrastructures du téléphone mobile permet de pallier la faiblesse de celles du téléphone fixe, plus coûteuses à déployer. En Afrique, le taux de pénétration du téléphone mobile est passé de 10 % à 70 % en sept ans, et il est estimé qu'en 2015, 69 % des Africains seront équipés de smartphones[52]. Il existe une forte corrélation entre expansion de l'internet mobile et pénétration d'internet dans les pays en développement et émergents. Selon l'étude précitée d'*InternetServiceProviders*, sur le prochain milliard d'utilisateurs, la plupart seront issus de pays non occidentaux ; la Chine, l'Inde et l'Indonésie compteront à elles seules trois milliards d'internautes.

La même disponibilité pourrait se manifester dans les prochaines années pour l'acquisition d'objets connectés. Une enquête auprès de consommateurs américains a montré que 12 % étaient prêts à acquérir les lunettes connectées développées par *Google* (les *Google Glass*) et 28 % une montre connectée. En France, un sondage a montré que les objets connectés étaient déjà utilisés par près d'un quart des Français[53]. 84 % des personnes interrogées les considèrent comme un progrès, contre 12 % seulement qui y voient un danger en raison de la diffusion d'informations confidentielles. Les domaines dans lesquels le développement des objets connectés est le plus attendu sont ceux de la santé et de la sécurité.

Un multiplicateur de collaborations

Durant ses premières années, le *web* était le lieu de relations asymétriques entre les éditeurs de site et des visiteurs passifs : les internautes accédaient à l'information diffusée par les sites internet qu'ils visitaient, en n'agissant que de manière limitée sur le contenu de ces sites. Des forums et groupes de discussions existaient mais ne permettaient que des échanges de messages textuels. L'augmentation des débits de connexion a permis au début des années 2000 l'émergence de nouveaux services reposant sur l'interaction, la collaboration et le partage entre des utilisateurs qui ne sont plus passifs, mais qui contribuent au contenu ; c'est ce tournant qui a été qualifié de « *Web 2.0* », selon une expression de Tim O'Reilly[54].

Les illustrations de cette logique d'interaction sont nombreuses :

- Les services de partage de pair à pair, comme *Napster* qui fut le plus populaire d'entre eux avant de fermer sur décision de justice, *eMule* ou *BitTorrent*, permettent à des particuliers d'échanger des documents, des morceaux de

52. Chiffres cités par G. Babinet, *L'ère numérique, un nouvel âge de l'humanité*, Le Passeur, 2014.
53. Enquête réalisée par BVA pour le Syntec numérique, février 2014.
54. T. O'Reilly, "What is Web 2.0 ? Design Patterns and Business Models for the Next Generation of Software", septembre 2005

musique ou des vidéos. L'attractivité de ces services repose sur la gratuité et le catalogue potentiellement illimité constitué par l'agrégation des fichiers détenus par chaque particulier.

- Les plateformes de partage de contenus, comme *Instagram* et *Flickr* pour les photos ou *Youtube* et *Dailymotion* pour les vidéos, avaient au départ vocation à permettre le stockage et la diffusion à un cercle d'amis. La possibilité d'ouvrir les contenus à l'ensemble des internautes a toutefois changé la nature de ces services, qui sont devenus de véritables médias de masse à l'échelle mondiale[55].

- De nombreux services sont fondés sur l'agrégation des recommandations faites par les internautes. Cette agrégation peut être déterminante pour créer la confiance nécessaire à l'utilisation de certains services : ainsi, des sites de covoiturage comme *BlaBlaCar* ou d'hébergement chez des particuliers comme *Couchsurfing* utilisent les notes et commentaires laissés sur chacun ; un utilisateur ayant fait l'objet de commentaires négatifs n'a que très peu de chances d'être sollicité à nouveau.

- Les réseaux sociaux sont sans doute le service le plus emblématique du *Web 2.0.* À la différence des services cités ci-dessus, les réseaux sociaux n'ont pas de vocation prédéfinie, du moins les réseaux à caractère généraliste comme *Facebook* et *Twitter*[56] : les personnes inscrites peuvent s'en servir pour faire connaître divers aspects de leur vie personnelle, mais aussi comme d'une lettre d'informations, d'un outil de militantisme politique, d'un canal de marketing ou d'un instrument de construction de réseaux professionnels ; le terme « Amis » sur *Facebook* recouvre des réalités diverses. Cette relative indéfinition a sans doute contribué au succès de ces services.

De manière remarquable, des services parviennent à produire des connaissances fiables par l'interaction entre une multitude d'utilisateurs. L'encyclopédie en ligne *Wikipedia* en est l'exemple le plus connu : les pages sont créées, complétées et corrigées grâce à la collaboration bénévole des utilisateurs ; selon un article publié dans la revue *Nature*, le niveau d'exactitude atteint est proche de celui de *l'Encyclopaedia Britannica*[57]. Le site de cartographie *OpenStreetMap* complète les données de base fournies par le système GPS (*Global Positioning System*) par les informations fournies par les utilisateurs ; il est à certains égards plus précis que d'autres sites qui n'identifient pas, par exemple, des chemins en zone rurale. Le site *Ushahidi,* « témoin » en kenyan, a été créé dans le contexte des violences qui ont suivi les élections contestées de 2007 dans ce pays. Il permet de partager des informations en temps réel sur ce type de situations de crise, permettant aux habitants d'éviter les zones dangereuses ; il a par la suite été utilisé pour organiser les secours après le tremblement de terre à Haïti en 2010.

55. La vidéo la plus vue sur *Youtube*, le clip « *Gangnam Style* » du Sud-Coréen Psy, a été visionnée près de 2 milliards de fois.

56. D'autres réseaux sociaux sont construits au contraire pour servir une finalité bien définie : professionnelle pour *LinkedIn* ou *Viadeo*, d'échange et de soutien entre malades pour *PatientsLikeMe*.

57. J. Giles, « Internet Encyclopaedias go head to head », *Nature*, 2005. Cité par G. Babinet, *op. cit*.

Crowdsourcing, crowdfunding... : petit lexique de la cocréation

Le ***crowdsourcing***, qu'on peut traduire par « *alimentation par la foule* », consiste à faire produire le contenu par la collaboration des utilisateurs, qu'il s'agisse de bâtir une encyclopédie, de recommander des restaurants ou de signaler dans une ville les obstacles à l'accessibilité des personnes handicapées.

L'***open source*** est un modèle développé dans l'univers du logiciel, où l'on parle en français de « *logiciel libre* ». Il consiste à rendre accessible et modifiable par tous le code source d'un logiciel. Cette ouverture doit notamment permettre d'en corriger plus facilement les défauts. Certains logiciels très utilisés sont des logiciels libres : le système d'exploitation *Linux*, le navigateur *Firefox* de Mozilla ou l'application de calcul parallèle *Hadoop*, très présente dans le domaine du *Big Data*. Par extension, on peut parler d'*open source* dès lors qu'il y a mise en commun et amélioration collective : c'est le cas des standards techniques d'internet développés par l'*Internet Engineering Taskforce* (IETF) et le *World Wide Web Consortium* (3WC) ou des procédés de cryptographie. L'expression d'*open source* est même utilisée en matière de renseignement, pour désigner la pratique consistant à recueillir des informations à partir de sources accessibles en ligne : on parle alors de « *renseignement d'open source* » ou ROSO.

Le ***crowdfunding*** ou financement participatif est un mode innovant de financement de projets. Plutôt que de recourir à l'endettement ou à un nombre limité d'investisseurs, les porteurs de projet présentent leur initiative sur internet dans le but de recueillir une somme suffisante par l'addition d'une multitude de petites contributions. Ce modèle est porté par des plateformes spécialisées, telles que *Kickstarter*, *KisskissBankbank* ou *Kiva*. Le *crowdfunding* peut servir aussi bien à recueillir des financements caritatifs qu'à démarcher des investisseurs, qui sont alors intéressés aux résultats du projet à la mesure de leur contribution.

Les ***FabLabs*,** ou laboratoire de fabrication, ont été inventés dans les années 2000 par des chercheurs du Massachussetts Institue of Technology (MIT). L'idée consiste à rendre accessible à tous des moyens de production permettant de concevoir et de fabriquer une grande variété d'objets. L'apparition des imprimantes 3D et la chute rapide de leur coût a stimulé l'essor des *FabLabs* : le fichier servant à l'impression du produit peut être ouvert à la communauté des utilisateurs, chacun pouvant ainsi travailler à son amélioration. L'*International FabLab Association* recense aujourd'hui des milliers de *FabLabs* adhérant à la charte du MIT. En France, le Gouvernement a lancé en juin 2013 un appel à projets pour stimuler le développement des *FabLabs*.

Il existe une parenté entre la logique de cocréation et l'absence de but lucratif. Nombre des initiatives présentées ci-dessus ont été portées par des acteurs à but non lucratif, comme la fondation Mozilla pour *Firefox* ou le MIT pour les *FabLabs*. Le secteur non lucratif n'a cependant pas l'apanage de la cocréation. La liseuse *Kindle* d'*Amazon* fonctionne ainsi avec une version retravaillée d'*Android*, le système d'exploitation pour smartphone conçu et placé en *open source* par

Google. De manière plus générale, nombre de grandes entreprises à but lucratif du numérique savent tirer profit de l'intelligence collective de leurs utilisateurs à travers l'exploitation de leurs données (cf. *supra* 1.1.2) ; c'est peut-être ce qui les distingue d'entreprises plus anciennes du secteur informatique, éditeurs de logiciels ou fabricants de matériels, dont le modèle d'affaires est plus classique.

Un vecteur de participation et de transparence dans l'action des pouvoirs publics

Le secteur public n'est pas resté insensible aux vertus de la cocréation. Le numérique y favorise la mise en œuvre des principes de participation du public (a) et de transparence (b).

(a) Le principe de participation du public à l'élaboration des politiques qui le concernent n'est pas né du numérique, mais celui-ci s'est avéré d'une grande puissance pour le mettre en œuvre. S'agissant des consultations publiques, internet et les nouvelles techniques de communication contribuent largement à favoriser l'implication d'acteurs nouveaux : membres d'associations peu connues, médias alternatifs, groupes d'intérêt isolés, experts, simples citoyens. S'instaure ainsi une sorte de démocratie directe dont les outils numériques sont les vecteurs. Les schémas traditionnels de représentation politique et de communication par voie écrite et même audiovisuelle, sans être supprimés, sont bousculés. Les nouvelles techniques de communication peuvent remplir de multiples fonctions selon les objectifs poursuivis : recueil d'avis, participation à la décision, évaluation des politiques publiques. Le règlement de l'Assemblée nationale prévoit ainsi que le public peut commenter sur le site de l'Assemblée le contenu des études d'impact rédigées par les services ministériels. Au niveau local, l'utilisation de l'outil internet dans les pratiques de communication et d'action municipales est désormais fréquente. Il suscite un intérêt attentif et prudent des élus et un engouement certain des parties prenantes locales intéressées.

La loi française consacre aujourd'hui ce rôle. Ainsi, le code de l'environnement prévoit une procédure électronique à l'article L. 120-1 inséré par la loi du 12 juillet 2010 dite *Grenelle II*. Une participation du public par internet peut lui permettre de réagir sur des projets d'aménagement qui ont une incidence directe sur l'environnement. De façon plus générale, la loi n° 2011-525 du 12 mai 2011 de simplification et d'amélioration de la qualité du droit prévoit qu'une consultation ouverte sur internet peut se substituer aux consultations obligatoires faites en application de dispositions législatives et réglementaires.

(b) Le principe de transparence dans l'action des pouvoirs publics a lui aussi des racines anciennes. Selon l'article 15 de la Déclaration des droits de l'homme et du citoyen, les citoyens ont le droit « *de demander compte à tout agent public de son administration* ». La loi du 17 juillet 1978 a instauré un principe de libre accès aux documents administratifs et permis aux particuliers de saisir une autorité administrative indépendante, la Commission d'accès aux documents administratifs (CADA), en cas de difficulté d'accès à un document. Cependant, l'information sur l'activité des pouvoirs publics susceptible d'être portée par le numérique prend

désormais une autre dimension : indépendamment des demandes des particuliers, l'ensemble des données concernant cette activité est susceptible d'être mis en ligne. C'est le mouvement de l'ouverture des données publiques, ou *Open Data*, qui vise plusieurs objectifs. Du point de vue de la vie démocratique, l'ouverture des données publiques ouvre à tout citoyen ou à tout groupement un droit de regard sur les moyens et les résultats des politiques publiques, lui permettant de dénoncer des dysfonctionnements, voire de contribuer à leur résolution. Du point de vue économique, de nombreux services peuvent être proposés grâce à l'exploitation des données publiques. Des portails nationaux de données publiques ont été créés dans de nombreux pays, notamment aux États-Unis, au Royaume-Uni et en France ; le portail www.data.gouv.fr, créé en 2012, est géré par un service du Premier ministre, la mission Etalab. Le principe de libre réutilisation des données publiques a été inscrit dans le droit de l'Union européenne par la directive 2003/98/CE du 17 novembre concernant la réutilisation des informations du secteur public, dite « *directive ISP* », transposée en France par une ordonnance du 6 juin 2005.

Un impact qui fait débat sur les normes sociales en matière de vie privée

Les possibilités nouvelles d'interaction ouvertes par le numérique changent nos modes de vie. Elles suscitent des débats sur l'évolution des normes sociales qu'elles impliqueraient en matière de vie privée. Ces débats opposent les tenants de la fin de la vie privée à ceux qui soutiennent que l'aspiration à la vie privée n'a pas disparu mais évolué.

Au cours des dernières années, les dirigeants de grandes entreprises du numérique ont multiplié les déclarations remettant en cause la pertinence du droit à la vie privée. Selon Eric Schmidt, alors président-directeur général de *Google*, « *si vous avez quelque chose à cacher, c'est peut-être que vous n'auriez pas dû le faire* »[58]. Vinton Cerf, « *chief evangelist* » de *Google* et l'un des concepteurs du protocole TCP/IP, a déclaré que « *la vie privée était peut-être une anomalie* »[59] : selon lui, l'idée de vie privée est née avec la révolution industrielle au XIXe siècle et à l'avenir, les évolutions des usages sociaux liés aux technologies numériques pourraient la rendre de plus en plus difficile à garantir. Marc Zuckerberg, président de *Facebook*, soutient de même que les normes sociales ont évolué et que son entreprise n'aurait fait que les suivre et s'y adapter[60].

---

58. Interview pour la chaîne américaine CNBC, décembre 2009.

59. Audition par la *Federal Trade Commission* (FTC), novembre 2013.

60. Interview par la revue en ligne *Tech Crunch*, janvier 2010. Marc Zuckerberg : « *En effet, il est intéressant de regarder en arrière, parce que quand nous avons commencé, dans ma chambre d'étudiant à Harvard, la question que beaucoup de gens se posaient était : 'Dans tous les cas, pourquoi voudrais-je mettre de l'information sur Internet ?' Et puis, enfin, cinq ou six ans après, vous savez, le blogging a décollé d'une manière considérable, et tous ces différents services qui font en sorte que les usagers partagent toutes ces informations. Les gens désormais se disent satisfaits non seulement de partager plus d'informations et de différents types, mais de façon plus ouverte et avec plus de monde. Cette norme sociale est tout simplement quelque chose qui a évolué au fil du temps.* » (…) « *Pour nous, notre rôle est d'adapter constamment notre système pour qu'il reflète ce que sont les normes sociales actuelles* ». Traduction de A. Casilli, « Contre

Ces thèses ne sont pas l'apanage des dirigeants de ces entreprises. Un journaliste américain, Jeff Jarvis, a forgé le concept de « *publicness* »[61] pour qualifier la valeur collective apportée selon lui par les pratiques de révélation de soi : la *publicness*, ou « publicisation de soi », permet de nouer des relations avec les autres, facilite la collaboration, crée la confiance et facilite l'identification des individus malveillants. Les réglementations destinées à protéger le droit à la vie privée, la *privacy*, risquent d'entraver les bénéfices collectifs de la *publicness*. L'évolution des attitudes à l'égard de la vie privée est parfois comparée à la révolution sexuelle des années 1960[62] : les attitudes désinhibées des jeunes générations suscitent la réprobation de leurs aînés, qui n'en mesurent pas la dimension libératrice ; comme pour la révolution sexuelle, cette liberté présente des risques que les individus devront apprendre à maîtriser, mais ses avantages sont perçus comme excédant ses inconvénients.

Ces thèses relatives à la spontanéité et au caractère librement consenti du dévoilement de soi sont contestées. Selon Antonio Casilli, chercheur en sociologie[63], les entreprises du numérique ne se contentent pas de refléter un changement de normes sociales mais agissent pour le faire advenir, car il correspond à leur intérêt financier ; elles se comportent en « *entrepreneurs de morale* », concept forgé par le sociologue Howard Becker pour qualifier les acteurs se mobilisant dans le but de changer la définition de ce qu'est un comportement déviant. Depuis sa création, *Facebook* a ainsi constamment élargi le périmètre des données qui sont visibles par tous dans les réglages par défaut. Le comportement des internautes serait loin de manifester une volonté totale de transparence sur soi-même et tendrait au contraire à faire un choix de plus en plus conscient entre ce qui est rendu public et ce qui est dissimulé, ces éléments pouvant varier selon les contextes. Antonio Casilli en déduit que l'aspiration à la vie privée n'a pas disparu mais qu'elle s'est transformée. Le droit à la vie privée ne peut plus seulement être compris comme le droit d'être protégé des intrusions d'autrui, le « *droit d'être laissé en paix* » (« *right to be left alone* ») que défendaient Samuel D. Warren et Louis D. Brandeis dans leur article fondateur de 1890[64]. L'enjeu devient, dans cette perspective, la maîtrise de la projection de soi dans les interactions sociales avec autrui, la vie privée impliquant aujourd'hui une « *négociation de soi* ». De même, face à la multiplication des traces laissées en ligne par les individus, qui dessinent une image de la personne accessible à tous les internautes, la volonté de contrôler sa « *e-réputation* » se développe.

---

l'hypothèse de la 'fin de la vie privée' », *Revue française des sciences de l'information et de la communication*, 2013, http://rfsic.revues.org/630.

61. J. Jarvis, *Public parts : How sharing in the digital age improves the way we work and live*. Simon & Schuster, 2011.

62. Cf. par exemple D. Peppers et M. Rogers, « The social benefits of data sharing », http://www.1to1media.com/View.aspx?DocId=31350, janvier 2009.

63. V. notamment *Les liaisons numériques*, Seuil, Paris, 2010, et la contribution à cette étude : « Quelle vie privée à l'ère du numérique ? », p. 423.

64. S. Warren et L. Brandeis, « The Right to Privacy », *Harvard Law Review*, vol. 4, 15 décembre 1890, n° 5.

Les adolescents et les réseaux sociaux : le point de vue d'une sociologue[65]

La plupart des adolescents utilisent quotidiennement les réseaux sociaux[66], tels que *Facebook, Twitter*, *Instagram* ou, plus récemment, *Snapchat*. Ces sites ou applications, qui leur permettent de se divertir et de communiquer entre eux exposent également leur vie privée.

Tout d'abord, il faut souligner que les préoccupations des adolescents et leur relation à la vie privée sont sensiblement les mêmes entre le monde réel et le monde virtuel :
- les réseaux sociaux sont pour eux un espace public et de liberté multipliant les opportunités de socialisation, et dans lequel ils construisent leur identité, de la même façon que dans le monde réel ;
- ils se préoccupent sincèrement de leur intimité, mais sans particulièrement se soucier des acteurs organisationnels, tels de potentiels employeurs, et sans renoncer à s'exprimer en public.

Cependant, la mise en réseau engendre une démultiplication des risques par rapport au monde réel :
- ils doivent maîtriser leur représentation personnelle devant un public disparate, qui va au-delà de leur cercle d'amis *(« invisible audience ») ;*
- ils doivent s'adresser simultanément à différents contextes sociaux, enracinés dans des normes différentes et exigeant à cet égard des réponses sociales différentes *(« collapsed contexts»)* ;
- ils doivent maîtriser une représentation personnelle construite par des tiers, produit des informations partagées par leurs relations.

De plus en plus conscients de ces risques, ils mettent en œuvre des stratégies de navigation sur ces réseaux :
- ils développent des compétences techniques pour mieux appréhender l'outil numérique, apprennent à maîtriser les paramètres de confidentialité des sites qu'ils utilisent (qui restent *« Public by Default »*) et cherchent à utiliser de nouvelles applications plus soucieuses de leur intimité[67] ;
- ils construisent une véritable « stéganographie sociale », qui utilise des outils linguistiques et culturels propres pour coder leurs messages, et les rendre incompréhensibles pour une personne extérieure.

En conclusion, les adolescents sont, plus qu'il n'y paraît, des internautes comme les autres. Cependant, leur maîtrise de l'environnement numérique et de ses codes n'est pas innée, et leur besoin de protection réel.

---

65. D. Boyd, *It's complicated, The Social Lives of Networked Teens*, 2014, http://www.danah.org/books/ItsComplicated.pdf. L'encadré résume quelques unes des principales conclusions de cette étude.

66. Un sondage mené en 2009 par l'institut *Common Sense Media* aux États-Unis démontre que 51 % des adolescents se connectent à leur réseau social favori au moins une fois par jour et que 22 % des jeunes le font plus de dix fois quotidiennement.

67. Selon une étude de *iStategyLabs*, 10 millions d'adolescents de moins de 18 ans ont quitté *Facebook* depuis 2011.

1.2. Le numérique a suscité la reconnaissance de nouveaux droits fondamentaux : le droit à la protection des données personnelles et le droit d'accès à internet

Le droit à la protection des données personnelles (1.2.1) et le droit d'accès à internet (1.2.2) sont nés en réponse aux questions posées par l'essor du numérique. S'ils sont souvent présentés comme se rattachant respectivement au droit à la vie privée et à la liberté d'expression, leurs enjeux sont en réalité plus larges ; ils peuvent donc être considérés comme des droits fondamentaux autonomes.

1.2.1. Le droit à la protection des données personnelles : un cadre juridique stable confronté à des enjeux radicalement nouveaux

Dans sa courte histoire, le droit à la protection des données personnelles aura connu un bouleversement complet des enjeux qui y sont associés.

Les recommandations du rapport Tricot, du nom du conseiller d'État, rapporteur général de la Commission informatique et libertés mise en place en novembre 1974 auprès du garde des sceaux, rapport remis le 27 juin 1975 au Premier ministre, ont servi de base à la loi du 6 janvier 1978 dite *informatique et libertés.* Elles ne pouvaient alors envisager ni l'essor d'internet, ni la puissance de calcul dont disposeraient des terminaux mobiles, ni la valeur économique acquise par les données, qu'elles soient ou non personnelles. Le cadre légal issu des recommandations du rapport s'est pourtant avéré d'une grande stabilité, ne donnant lieu qu'à une seule réforme importante, intervenue pour transposer la directive n° 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995.

La loi du 6 janvier 1978, texte fondateur, a été la première à reconnaître ce droit

La loi du 6 janvier 1978 reste associée dans les mémoires collectives à l'émotion suscitée par le projet « *Safari* » (pour Système automatisé pour les fichiers administratifs et le répertoire des individus), révélée par le quotidien *Le Monde* dans un article intitulé « Safari ou la chasse aux Français »[68]. L'article de Philippe Boucher mettait en évidence un projet de rassemblement de fiches dispersées dans différents services de police, ainsi qu'une volonté d'interconnexion avec les fichiers du cadastre, des impôts et du ministère du travail. Le numéro d'inscription au répertoire d'identification des personnes physiques géré par l'INSEE, attribué à chaque personne résidant sur le territoire français, aurait servi d'identifiant unique permettant cette interconnexion. En réaction à cette affaire, une circulaire du Premier ministre du 29 mars 1974 interdisait à titre conservatoire toute nouvelle interconnexion entre des systèmes informatiques relevant de ministères différents

68. *Le Monde*, 21 mars 1974.

et un décret du 8 novembre 1974 constituait auprès du garde des sceaux une commission informatique et libertés, présidée par Bernard Chenot, vice-président du Conseil d'État, et par Maurice Aydalot, premier président de la Cour de cassation, Bernard Tricot en étant rapporteur général.

Des travaux avaient cependant précédé ce rapport. En 1969, le Conseil d'État avait déjà conduit une réflexion sur « *les conséquences du développement de l'informatique sur les libertés publiques et privées et sur les décisions administratives* » (rapport annuel de 1969-1970). Nombre de ses constats restent d'une grande actualité : « *Certes il n'y a rien de nouveau dans le fait de chercher à s'informer, de collecter à cette fin des renseignements et de les rapprocher de la façon la mieux adaptée à la fin poursuivie. Mais l'efficacité sans précédent de la machine transforme cette activité non seulement dans ses dimensions, mais aussi dans sa nature. Elle permet un regroupement presque illimité, elle conserve indéfiniment, elle n'oublie jamais ; elle restitue l'information stockée sans peine, elle permet le rapprochement de renseignements aujourd'hui inexistants ou épars* ». Annonçant que « *les Français vont donc vivre dans une civilisation de l'information* », où « *la recherche de l'information devient une activité rentable, sa détention une source de puissance* », l'étude identifiait déjà le risque de la constitution de « *banques de données* », où les informations de toute nature concernant un individu seraient regroupées. Par ailleurs, plusieurs pays étrangers avaient adopté au début des années 1970 des lois de protection des données: la Suède, en 1973 ; les États-Unis, avec une loi concernant les données bancaires en 1970 (*Fair Credit Reporting Act*) et une autre loi concernant les données administratives en 1974 (*Privacy Act*) ; la République fédérale d'Allemagne, avec des lois de protection des données dans les Länder de Hesse, de Bavière et de Rhénanie-Palatinat.

La loi du 6 janvier 1978 a fait trois choix fondamentaux : elle a retenu une approche transversale, couvrant l'ensemble des données personnelles (alors qualifiées « *d'informations nominatives* ») ; elle reconnaît à la personne des droits sur les informations qui la concernent ; elle crée une autorité administrative indépendante chargée de veiller à sa mise en œuvre, la Commission nationale de l'informatique et des libertés (CNIL).

L'article 4 de la loi définit un champ d'application général : selon ses termes, « *les informations qui permettent, sous quelque forme que ce soit, directement ou non, l'identification des personnes physiques auxquelles elles s'appliquent, que le traitement soit effectué par une personne physique ou par une personne morale* ». Aucune des dispositions de la loi ne prévoit un encadrement particulier pour certains types de traitements ou secteurs d'activité, si ce n'est pour réserver aux autorités publiques le traitement automatisé des informations nominatives concernant les infractions, condamnations ou mesures de sûreté (article 30). Les traitements des secteurs public et privé sont couverts, même si c'était alors avec un régime juridique nettement différencié. Cette approche généraliste, qui se retrouve aujourd'hui dans les textes européens, tranche avec l'approche sectorielle que les États-Unis avaient adoptée dès cette époque et qu'ils ont maintenue par la suite.

Le droit américain de la protection des données personnelles : un cadre substantiellement différent du droit européen[69]

Le cadre juridique américain diffère substantiellement de celui de l'Union européenne. Trois différences majeures peuvent être soulignées : le droit américain résulte de lois sectorielles et non d'un cadre général (a) ; il retient une approche subjective, centrée sur la réparation du préjudice subi (b) ; il fait une large place à l'autorégulation (c). En raison de l'ampleur des échanges commerciaux entre les États-Unis et l'Union européenne, des influences réciproques s'exercent cependant entre les deux zones (d).

a) Le cadre juridique américain résulte d'une juxtaposition de lois particulières. Dans le secteur public, le *Privacy Act* de 1974 prescrit d'appliquer des pratiques d'information « justes » définies dans le *Code of Fair Information Practices*. Cinq pratiques sont identifiées : interdiction des systèmes secrets d'enregistrement des données ; possibilité d'accès pour l'intéressé à ces informations ; principe de limitation de la finalité (sauf accord préalable) ; possibilité de correction des informations ; principe de sécurité des informations. Le *Privacy Act* identifie en outre une catégorie particulière de données sensibles : « *les fichiers décrivant comment un individu exerce des droits garantis par le Premier amendement*[70] » . De tels fichiers ne seront en principe pas conservés, sauf à prévoir un encadrement « strict » et « pertinent ». Dans le secteur privé, seuls certains types de données font l'objet d'une protection législative : données des communications électroniques (*Electronic Communication Privacy Act* de 1986), données de santé (*Health Insurance Portability and Accountability Act* de 1996), données en ligne concernant les mineurs (*Children's Online Privacy Protection Act* de 1998) et données financières (*Fair Credit Reporting Act* de 1970 et *Gramm-Leach Billey Act* de 1999).

Certes, le quatrième amendement à la Constitution[71] fonde une protection générale de la vie privée, indépendamment de tout cadre législatif. Toutefois, l'interprétation de ses termes peut être délicate face aux développements technologiques modernes. En outre, à la suite de l'arrêt *Katz*[72] de 1967, la Cour suprême a adopté une conception restrictive du droit à la vie privée garanti par

69. Encadré réalisé avec le concours de la cellule de droit comparé du centre de recherches et de diffusion juridiques (CRDJ) du Conseil d'État.

70. « *Le Congrès ne fera aucune loi pour conférer un statut institutionnel à une religion, qui interdise le libre exercice d'une religion, qui restreigne la liberté d'expression, ni la liberté de la presse, ni le droit des citoyens de se réunir pacifiquement et d'adresser à l'État des pétitions pour obtenir réparation de torts subis [sans risque de punition ou de représailles]* ».

71. « *Le droit des citoyens d'être garantis dans leurs personne, domicile, papiers et effets, contre les perquisitions et saisies non motivées ne sera pas violé, et aucun mandat ne sera délivré, si ce n'est sur présomption sérieuse, corroborée par serment ou affirmation, ni sans qu'il décrive particulièrement le lieu à fouiller et les personnes ou les choses à saisir.* »

72. *Katz v. États-Unis* (1967) 389 U.S. 347, p. 361.

le quatrième amendement, en définissant le « *test des attentes raisonnables* » (« *reasonable expectations* »). Pour qu'il y ait un droit à la vie privée garanti par la Constitution, une personne doit « *avoir formulé une attente réelle en matière de protection de la vie privée* » et « *l'attente [doit] être une attente que la société est prête à reconnaître comme raisonnable* ». Dans l'affaire dite du *Pen Register*[73] (enregistreur graphique), la Cour suprême a jugé que les utilisateurs de téléphone pouvant raisonnablement s'attendre à ce que les compagnies de téléphone enregistrent les numéros appelés, cet enregistrement ne méconnaît pas le quatrième amendement. En revanche, la Cour a jugé dans une autre affaire[74] que l'utilisation par le gouvernement d'un imageur thermique sans mandat est illégale, faute pour cette technologie d'être utilisée par le grand public.

b) Le modèle américain est essentiellement fondé sur des principes de réparation délictuelle et contractuelle. Il tend à réparer le préjudice subi par les consommateurs et vise à obtenir un équilibre entre l'atteinte à la vie privée et à la libre circulation des données. La preuve d'un préjudice ou d'un risque de préjudice n'est pas toujours aisée à apporter. Dans un arrêt *Krottner v. Starbucks*[75], la cour d'appel du 9e circuit a jugé que des employés de l'entreprise *Starbucks*, qui se plaignaient du vol de leurs numéros de sécurité sociale détenus par l'entreprise, avaient bien démontré l'existence d'une « *menace crédible de préjudice réel et sérieux résultant du vol de l'ordinateur et de ses données à caractère personnel encryptées* ». En revanche, dans une affaire similaire *Reilly v. Ceridian*, la cour d'appel du 3e circuit a rejeté la requête des plaignants en considérant que leurs affirmations reposaient simplement sur la spéculation que le pirate avait lu, copié et compris les données personnelles volées.

c) Dans le cadre de l'effort d'autoréglementation encouragé par le Gouvernement, des acteurs privés (entreprises, associations, etc.) non visés par les législations spécifiques ont volontairement décidé d'adopter une politique relative à la protection des données personnelles. La *Federal Trade Commission* (FTC) a mis en place un code de bonnes pratiques, mais qui n'est que facultatif. Ce modèle d'autoréglementation diffère du système européen, mais aussi de l'Australie et du Canada, qui imposent des *fair information practices* aux acteurs privés.

d) Les systèmes européen et américain tendent cependant à s'influencer de manière réciproque, en raison de l'ampleur des échanges entre les deux zones. La directive européenne du 24 octobre 1995 a dans une certaine mesure une portée extraterritoriale, puisqu'elle interdit en principe les transferts de données des Européens vers des États tiers n'assurant pas un « *niveau de protection adéquat* ». Certains auteurs évoquent même un « *Brussels Effect* »[76] pour désigner cette influence de la réglementation européenne.

73. *Smith v. Maryland* (442U.S. 735, 1979).
74. *Kyllo v. États-Unis* (533, U.S. 141, 2000).
75. *Krottner v. Starbucks Corp.*, 628 F.3d 1139, 1140 (9th Cir. 2010).
76. Ann Bradford, « *The Brussels Effect* », 107 *Nw. U. L. REV.* I (2012).

Dans la période récente, plusieurs initiatives ont été prises pour renforcer la protection des données personnelles aux États-Unis. La Maison Blanche a présenté en 2012 un projet de loi, le *Consumer Privacy Bill of Rights*[77], qui imposerait le respect d'un certain nombre de principes (contrôle de leurs données par les individus, transparence, respect du contexte dans lequel les données ont été collectées, sécurité, droit d'accès, limites raisonnables à la collecte et à la conservation, « *accountability* » des entreprises) à l'ensemble des entreprises traitant les données des consommateurs. Il renvoie à une démarche de corégulation avec les entreprises pour la mise en œuvre de ces principes dans les différents contextes professionnels. Si ce texte était adopté, les États-Unis se doteraient ainsi pour la première fois d'un instrument transversal et non sectoriel en matière de protection des données personnelles. L'absence de majorité démocrate à la Chambre des représentants a cependant fait obstacle à ce jour à son adoption. Un autre projet de loi a été déposé par les sénateurs Jay Rockefeller et Edward Markey[78] pour accroître la transparence sur les pratiques des *data brokers* (courtiers en données personnelles) ; celles-ci seront présentées plus longuement dans la deuxième partie (cf. *infra* 2.1.1).

La loi du 6 janvier 1978 institue des droits des personnes sur les données qui les concernent. Ceux-ci peuvent être classés en deux catégories : les droits concernant la constitution des fichiers et ceux relatifs à l'utilisation de ces fichiers pour prendre des décisions. S'agissant de la première catégorie, les personnes ont un droit d'opposition à ce que des données qui les concernent fassent l'objet d'un traitement, sauf lorsque le traitement répond à une obligation légale ou lorsque ce droit a été expressément écarté par l'acte autorisant le traitement ; un droit d'information, notamment sur les personnes physiques ou morales destinataires des informations recueillies ; un droit d'accès, dans le but de savoir si un traitement comporte des informations qui les concernent et si oui, d'en avoir communication ; un droit de rectification, selon lequel l'individu « *peut exiger que soient rectifiées, complétées, clarifiées, mises à jour ou effacées les informations le concernant qui sont inexactes, incomplètes, équivoques, périmées ou dont la collecte, ou l'utilisation, la communication ou la conservation est interdite* ». Les droits de la seconde catégorie, d'ailleurs placés en tête de la loi puisqu'ils figurent aux articles 2 et 3, ont pour but d'éviter un recours aveugle à l'informatique, susceptible de donner aux décisions issues de sa mise en œuvre un caractère prétendument incontestable. Ce risque avait été souligné par le rapport Tricot, qui qualifiait de « *démission* » le fait de « *s'en remettre entièrement à [l'informatique] pour*

77. Ce projet de loi a été présenté dans le cadre du rapport de la Maison Blanche : *Consumer Data Privacy in a Networked World : A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy*, février 2012. Cf. aussi sur le même sujet aux États-Unis *Federal Trade Commission, Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers*, 2012; Executive Office of the President, *Big Data : Seizing Opportunities, Preserving Values*, mai 2014.

78. *Data Broker Accountability and Transparency Act*, février 2014.

apprécier des situations humaines »[79]. La loi proscrit le profilage automatique, c'est-à-dire la prise d'une décision impliquant une appréciation sur un comportement humain sur le fondement d'un algorithme établissant le profil d'un individu : cette interdiction est stricte pour les décisions de justice, qui ne peuvent se fonder sur un tel traitement automatisé ; pour les décisions administratives ou privées, il interdit seulement que le traitement automatisé soit le seul fondement. Elle prévoit aussi que « *toute personne a le droit de connaître et de contester les informations et les raisonnements utilisés dans les traitements automatisés dont les résultats lui sont opposés* » ; il s'agit d'éviter que l'informatique ne fonctionne, selon une formule courante, comme une « *boîte noire* ».

Conformément aux préconisations du rapport Tricot, la loi crée une instance originale pour veiller à sa mise en œuvre, la CNIL. Cette originalité tient autant à ses missions qu'à son statut. La loi lui confie une large gamme de missions : elle lui confère un rôle d'information des personnes, d'autorisation des traitements mis en œuvre pour le compte des personnes publiques, de contrôle et de vérification, ainsi qu'un pouvoir réglementaire dans les cas qu'elle définit. S'agissant du statut, le projet de loi adopté par le conseil des ministres ne prévoyait pas expressément l'indépendance de la CNIL. Si le rapport Tricot préconisait que l'instance de contrôle « *jouisse d'une grande indépendance juridique et morale* »[80], il ne consacrait pas de développements à la teneur de cette indépendance et à ses garanties ; la notion d'autorité administrative indépendante n'avait alors pas la consistance que plusieurs lois successives et la réflexion doctrinale allaient ultérieurement lui donner[81]. L'affirmation de l'indépendance de la Commission est le fruit de la discussion parlementaire. Le rapport fait au nom de la commission des lois du Sénat souligne ainsi que « *tout l'effort de la commission a tendu (…) à laisser à la commission son caractère d'autorité administrative tout en lui conférant, notamment par sa composition, l'autorité et l'indépendance requises pour pouvoir accomplir sa mission* » [82]. La loi du 6 janvier 1978 dispose que la CNIL est une « *autorité administrative indépendante* ». Il ne peut être mis fin aux fonctions de ses membres qu'en cas de démission ou d'empêchement constaté par la Commission, et les membres ne peuvent recevoir d'instruction d'aucune autorité.

Plus de trente-cinq ans après le vote de la loi, ces trois choix structurent toujours le cadre français de la protection des données personnelles et se retrouvent dans les instruments de droit européen et international. Le choix d'une forte différenciation de l'encadrement des traitements selon qu'ils sont mis en œuvre pour le compte de personnes publiques ou privées apparaît en revanche plus daté. La loi du 6 janvier 1978 est née de préoccupations liées à l'utilisation de l'informatique par les pouvoirs publics. Le rapport Tricot avait consacré de plus longs développements à l'informatique publique qu'à son utilisation par les entreprises, *a fortiori* à celle des

79. Cf. sur la genèse de la notion, Conseil d'État, *Les autorités administratives indépendantes, rapport public 2001*, Paris, La documentation Française.

80. *Ibid*, p. 74.

81. Cf. sur la genèse de la notion, Conseil d'État, *Les autorités administratives indépendantes*, rapport public 2001, Paris, La documentation Française.

82. Sénat, rapport fait au nom de la commission par M. Jacques Thyraud, n° 72, p. 25.

particuliers qui était quasi inexistante. En conséquence, la loi soumet à un régime d'autorisation les traitements d'informations nominatives mis en œuvre pour le compte des personnes publiques ou des personnes privées chargées d'une mission de service public (sont notamment visés les organismes de sécurité sociale) : ils doivent être décidés par un acte réglementaire pris après avis de la CNIL ; si cet avis est défavorable, seul un décret pris sur avis conforme du Conseil d'État peut autoriser le traitement. Ce régime exorbitant – il s'agit du seul cas dans lequel les avis du Conseil d'État lient le Gouvernement – traduit la méfiance à l'égard du développement de l'informatique publique. Autre illustration de cette méfiance, l'utilisation du répertoire national d'identification des personnes physiques (RNIPP) géré par l'INSEE, où sont consignés les numéros d'inscription au répertoire (NIR), dits couramment « numéros INSEE » ou « numéro de sécurité sociale », doit être autorisée par décret en Conseil d'État pris après avis de la CNIL. Les traitements mis en œuvre pour le compte de personnes privées ne sont en revanche soumis qu'à une obligation de déclaration.

Ce droit fondamental a été consacré successivement par le droit international, le droit de l'Union européenne et la jurisprudence constitutionnelle

L'évolution du droit international et de la jurisprudence constitutionnelle a permis d'inscrire le droit à la protection des données personnelles à un niveau supérieur à celui de la loi dans la hiérarchie des normes. Ceci permet au juge d'exercer son contrôle y compris à l'égard de traitements de données prévus par des textes législatifs.

• *Le droit à la protection des données personnelles dans le droit international et le droit de l'Union européenne*

Le droit à la protection des données personnelles est aujourd'hui garanti tant par des instruments spécifiques que par des conventions générales relatives aux droits de l'homme.

Le Conseil de l'Europe a adopté le 28 janvier 1981 la convention n° 108 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel. L'approche adoptée par cette convention présente de fortes similitudes avec la loi française du 6 janvier 1978 : champ d'application général, couvrant tous les traitements automatisés de données à caractère personnel des secteurs public et privé ; reconnaissance de droits d'information, d'accès, de rectification et de recours ; prohibition de la collecte des données qui révèlent « *l'origine raciale, les opinions politiques, les convictions religieuses ou autres convictions, ainsi que les données à caractère personnel relatives à la santé ou à la vie sexuelle (…) à moins que le droit interne ne prévoie des garanties appropriées* ». L'article 5 de la convention introduit une notion qui ne figurait pas dans la loi du 6 janvier 1978, celle de « *qualité des données* », qui recouvre cinq principes : loyauté de la collecte ; enregistrement pour des finalités « *déterminées et légitimes* » ; proportionnalité des données collectées par rapport à ces finalités ; exactitude des données ; durée de conservation proportionnée aux finalités. L'influence

des lignes directrices de l'OCDE régissant la protection de la vie privée et les flux transfrontières de données de caractère personnel, adoptées sous forme d'une recommandation du Conseil de l'OCDE le 23 septembre 1980, doit sur ce point être notée. Ces lignes directrices ont sans doute elles-mêmes été inspirées par le *Code of Fair Information Practices* américain de 1973, intégré au *Privacy Act* de 1974, qui prévoit notamment le principe de collecte pour des finalités déterminées ; compte tenu de sa composition, l'OCDE a été un lieu de rapprochement entre les positions américaines et européennes. La convention n° 108 a été ratifiée par 45 des 47 États membres du Conseil de l'Europe, seuls la Turquie et Saint-Marin n'y étant pas parties. Elle a recueilli au cours des quinze dernières années un nombre significatif de ratifications, notamment de pays d'Europe orientale non membres de l'Union européenne (Albanie, Arménie, Géorgie, Russie, Serbie, Ukraine, etc.), ce qui témoigne de son pouvoir d'attraction. La convention n° 108 est également ouverte à la ratification d'États non membres du Conseil de l'Europe ; l'Uruguay est devenu en 2013 le premier de ces États non membres parties à la convention.

La directive n° 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données est le fruit d'une double volonté, que traduit bien son intitulé : protéger les droits des personnes et favoriser la libre circulation de ces données. Elle était motivée par les enjeux économiques croissants liés aux échanges transfrontaliers de données, que les différences de législation entre les États européens étaient susceptibles d'entraver. C'est d'ailleurs uniquement ce dernier objectif qui fondait juridiquement la compétence de la Communauté européenne : la directive a été prise sur le fondement de l'article 100 A du traité (aujourd'hui article 114 du Traité sur le fonctionnement de l'Union européenne (TFUE)), relatif au rapprochement des législations des États membres ayant pour objet l'établissement et le fonctionnement du marché intérieur. Comme l'a souligné le président Guy Braibant, « *il n'était pas évident que cette question relève de la compétence de la Communauté, qui n'avait pas mission de s'occuper de protection des libertés et de la vie privée* »[83]. Au cours des travaux préparatoires à son adoption, l'Assemblée nationale et le Sénat, par des résolutions prises sur le fondement de l'article 88-4 de la Constitution, ainsi que le Conseil d'État[84], saisi d'une demande d'avis par le Gouvernement, ont souligné que l'intervention de la Communauté européenne ne pouvait être admise que si elle n'avait pas pour effet d'affaiblir la protection des personnes assurées par la loi du 6 janvier 1978.

En dépit des réserves alors formulées, liées à la motivation économique de la directive, celle-ci reprend l'approche de protection des droits fondamentaux des lois de plusieurs États membres, dont la loi française, et de la convention n° 108 du Conseil de l'Europe. Son champ d'application est général et couvre les secteurs publics et privés. Les principes relatifs à la qualité des données, fixés par l'article 6, sont

83. G. Braibant, *Données personnelles et société de l'information*, rapport au Premier ministre sur la transposition de la directive n° 95/46, p. 32, mars 1998.

84. Résolutions du 25 juin 1993, pour l'Assemblée nationale, et du 7 juin 1994, pour le Sénat. Avis du Conseil d'État du 10 juin 1993, cf. *Les grands avis du Conseil d'État,* Dalloz, 2008, pp. 239-244.

identiques à ceux prévus par la convention n° 108. Les droits d'information, d'accès, d'opposition et de rectification sont garantis dans des termes similaires, ainsi que le droit de ne pas être soumis à une décision individuelle prise sur le seul fondement d'un traitement automatisé. Le traitement de données qui révèlent l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques, l'appartenance syndicale, ainsi que le traitement des données relatives à la santé et à la vie sexuelle, sont en principe prohibés. En outre, à la différence de la convention n° 108 du Conseil de l'Europe, la directive impose à chaque État la création d'une autorité de contrôle indépendante, dotée de pouvoirs d'investigation et d'intervention. Elle instaure un groupe européen des autorités nationales de protection des données (souvent dénommé « G29 », son existence étant prévue par l'article 29 de la directive), chargé notamment « *d'examiner toute question portant sur la mise en œuvre des dispositions nationales prises en application de la présente directive, en vue de contribuer à leur mise en œuvre homogène* ».

S'agissant des échanges transfrontaliers de données, la directive introduit une césure entre les échanges entre États membres de l'Union européenne et les échanges avec des États tiers. Les échanges intra-européens sont régis par un strict principe de libre circulation : en aucun cas, les États ne peuvent « *restreindre ni interdire la libre circulation des données à caractère personnel entre États membres* » pour des motifs tenant à la protection des droits fondamentaux des personnes physiques. Les transferts vers des pays tiers ne sont autorisés que si ce pays assure un « *niveau de protection adéquat* ». L'existence ou l'absence d'un niveau de protection adéquat est constatée par une décision de la Commission, prise après avis du G29. À ce jour, la Commission a reconnu que le niveau de protection était adéquat dans 11 États : Andorre, l'Argentine, l'Australie, le Canada, les îles Féroé, Guernesey, Israël, Jersey, la Nouvelle-Zélande, la Suisse et l'Uruguay. Deux décisions spécifiques ont été prises concernant les États-Unis, l'une ayant trait à l'accord du *Safe Harbour*, l'autre au fichier « *Passenger Name Record* » (PNR). Lorsque le pays tiers n'assure pas un niveau de protection adéquat, l'article 26 de la directive admet le transfert dans un certain nombre de cas : consentement indubitable de la personne concernée, transfert nécessaire à l'exécution d'un contrat, à la sauvegarde d'un intérêt public important, à la défense d'un droit en justice ou à la sauvegarde de l'intérêt vital de la personne concernée, garanties apportées par le responsable du traitement sous forme de « *clauses contractuelles appropriées* ».

Clauses contractuelles appropriées, *Safe Harbour* et autres régimes du transfert de données vers des États tiers

Clauses contractuelles appropriées : L'article 26.2 de la directive dispose qu'un État membre peut autoriser un transfert de données à caractère personnel vers un État tiers n'assurant pas un niveau de protection adéquat lorsque le responsable du traitement présente des garanties suffisantes, qui « *peuvent notamment résulter de clauses contractuelles appropriées* ». En France, l'article 69 de la loi du 6 janvier 1978 dispose que c'est la CNIL qui prend cette décision,

sauf pour les traitements intervenant dans les matières « régaliennes »[85], pour lesquels le transfert doit être autorisé par décret en Conseil d'État pris après avis de la CNIL.

L'article 26.4 de la directive permet à la Commission de reconnaître des « *clauses contractuelles types* », dont elle estime qu'elles présentent des garanties suffisantes ; cette décision s'impose aux États. Adoptées pour la première fois en 2001 puis modifiées à plusieurs reprises, les clauses contractuelles types définissent le contenu du contrat de transfert à conclure entre l'exportateur et l'importateur des données. Elles prévoient des obligations pour l'exportateur (information des personnes concernées et de l'autorité de contrôle) et pour l'importateur (respect de « *principes obligatoires de protection des données* » qui correspondent à ceux fixés par la directive, acceptation de vérifications par l'exportateur ou un organisme de contrôle, etc.).

Règles d'entreprises contraignantes : Les règles d'entreprises contraignantes (en anglais « *Binding Corporate Rules* » ou « *BCR* ») sont des codes de conduite internes adoptés par des entreprises multinationales afin d'encadrer les transferts de données de leurs entités situées dans l'Union européenne vers leurs entités situées en dehors de l'Union, dans des pays n'assurant pas un « *niveau de protection adéquat* » au sens de la directive. Cet instrument, qui n'est pas explicitement prévu par la directive, a été élaboré par le G29 sur le fondement de l'article 26.2, qui permet d'autoriser un transfert lorsque le responsable de traitement « *offre des garanties suffisantes* »[86] ; le G29 considère que des règles d'entreprises contraignantes établies selon le modèle qu'elle a défini peuvent présenter de telles garanties. Le projet de règles d'entreprises contraignantes doit être approuvé par l'autorité de contrôle pour que les transferts soient autorisés. Une entreprise établie dans plusieurs États membres peut choisir de présenter sa demande à une autorité « chef de file », qui accorde alors l'autorisation pour le compte de l'ensemble des autorités compétentes, après les avoir consultées.

Safe Harbour : L'article 25.5 de la directive permet à la Commission d'engager des négociations avec un État tiers n'assurant pas un niveau de protection adéquat, en vue de remédier à cette situation. C'est sur ce fondement que la Commission a engagé des négociations avec le département du commerce américain, qui ont abouti à ce que celui-ci publie le 21 juillet 2000 des « *Principles of Safe Harbour* » (principes de la « sphère de sécurité ») ainsi que des « *Frequently Asked Questions* » (questions fréquemment posées, ou « *FAQ* ») sur leur mise en œuvre. Par une décision n° 2000/520/CE du 26 juillet 2000, la Commission a constaté que ces principes assuraient un niveau de protection adéquat et

85. Il s'agit des matières énumérées au I de l'article 26 de la loi : sûreté de l'État, défense, sécurité publique, prévention, recherche, constatation ou poursuite des infractions pénales ou exécution des condamnations pénales ou des mesures de sûreté.

86. Article 29 Working Party, *Working Document: Transfers of personal data to third countries : Applying Article 26 (2) of the EU Data Protection Directive to Binding Corporate Rules for International Data Transfers*, juin 2003, 11639/02/EN WP 74.

permettaient donc le transfert de données vers des entreprises établies aux États-Unis, à condition que celles-ci s'engagent publiquement et clairement à respecter les principes mis en œuvre conformément aux FAQ, et qu'elles soient soumises aux pouvoirs légaux de contrôle de la *Federal Trade Commission* (FTC) ou du ministère des transports.

Les principes du *Safe Harbour* reprennent certaines des exigences de la directive n° 95/46/CE, telles que les droits d'information, d'accès et d'opposition ainsi que l'obligation de sécurité incombant au responsable du traitement. Toutefois, certains principes voient leur force atténuée : ainsi, en ce qui concerne les données sensibles (origine ethnique, religion, santé, etc.), les principes du *Safe Harbour* n'indiquent pas que leur traitement est en principe interdit, mais seulement que les personnes concernées doivent « *avoir positivement ou explicitement la possibilité de décider (consentement) si les données peuvent être divulguées à un tiers ou utilisées dans un but qui diffère de l'objectif initial de la collecte* ». Surtout, la mise en œuvre des principes repose sur une logique « d'auto-certification » : pour bénéficier du *Safe Harbour*, les entreprises doivent déclarer publiquement qu'elles y adhèrent, intégrer les principes dans leur politique interne relative à la vie privée (« *privacy policy* »), qui doit être publique et accessible, et remettre chaque année au département du commerce des documents certifiant l'application des principes. La FTC peut sanctionner les entreprises sur le terrain des pratiques commerciales trompeuses si elle constate que les principes ne sont pas effectivement mis en œuvre. En vertu de l'article 3.1 de la décision du 26 juillet 2000, les autorités nationales de protection des données des États membres de l'Union européenne peuvent, dans certains cas limitativement définis, suspendre les flux de données vers une entreprise adhérant au *Safe Harbour*.

À la suite des révélations sur les programmes de surveillance mis en œuvre par le gouvernement américain, ainsi qu'à des controverses concernant plus particulièrement le fonctionnement du Safe Harbour, la Commission s'est engagée dans une renégociation de celui-ci[87].

***Passenger Name Record* (PNR)** : Après les attentats du 11 septembre 2001, deux lois américaines[88] ont imposé aux compagnies aériennes de leur transmettre les données concernant les passagers ayant réservé un vol à destination des États-Unis. Dans un premier temps, la Commission a adopté, comme pour le *Safe Harbour*, une décision sur le fondement de l'article 25.6 de la directive du 24 octobre 1995, constatant l'existence d'un niveau de protection

87. Cf. deux communications de la Commission européenne en date du 27 novembre 2013 : « *Rebuilding Trust in EU-US Data Flows* », COM(2013) 846 ; « *On the Functioning of the Safe Harbour from the Perspective of EU Citizens and Companies Established in the EU* », COM(2013) 847.

88. *Aviation and Transportation Security Act* du 19 novembre 2001 et *Enhanced Border Security and Visa Entry Reform Act* du 5 mai 2002.

adéquat[89]. Saisie d'un recours par le Parlement européen, la Cour de justice des communautés européennes a annulé cette décision, au motif qu'elle était intervenue en dehors du champ d'application de la directive du 24 octobre 1995, qui exclut les traitements ayant pour objet la sécurité publique, la sûreté de l'État et le droit pénal[90]. Un nouvel accord a été signé avec les États-Unis le 26 juillet 2007, cette fois-ci dans le cadre de ce qui était avant le traité de Lisbonne le « troisième pilier » de l'Union européenne, relatif à la justice et aux affaires intérieures. Les transferts de données personnelles prévus par l'accord PNR interviennent donc en dehors du cadre de la directive du 24 octobre 1995.

Adoptée en 2000 lors du Conseil européen de Nice et dotée d'une portée contraignante depuis l'entrée en vigueur du traité de Lisbonne en décembre 2009, la Charte des droits fondamentaux de l'Union européenne reconnaît dans son article 8 le droit à la protection des données personnelles. L'article 8.2 reprend un certain nombre de principes figurant dans la directive du 24 octobre 1995 : traitement loyal, à des fins déterminées et sur la base du consentement de la personne ou d'un autre fondement légitime prévu par la loi, droit d'accès et de rectification. L'article 8.3 impose que le respect de ces règles soit « *soumis au contrôle d'une autorité indépendante* ». Ces principes sont ainsi placés au plus haut niveau de la hiérarchie des normes du droit de l'Union européenne : ils s'imposent aux institutions de l'Union et aux États membres lorsqu'ils mettent en œuvre le droit de l'Union. Il faut souligner que la Charte distingue le droit à la protection des données personnelles du droit au respect de la vie privée, protégé par l'article 7. Le commentaire de Guy Braibant, qui fut vice-président de la « *Convention* » chargée de l'élaboration de la Charte, explique ce choix par l'importance des enjeux de protection des données personnelles à l'époque contemporaine : « *avec la bioéthique, l'informatique est l'un des domaines importants des évolutions scientifiques et techniques du XXe siècle qui affectent la liste des droits fondamentaux* »[91]. Il peut également se justifier par le fait que la protection des données personnelles est certes une garantie pour le droit à la vie privée, mais aussi pour d'autres droits fondamentaux. En particulier, l'interdiction de traiter les données sensibles est une garantie pour la liberté d'expression, la liberté religieuse ou la liberté syndicale.

Texte plus ancien, la Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales ne comporte pas d'article dédié à la protection des données personnelles et c'est donc sur le fondement du droit au respect de la vie privée, prévu par l'article 8, que la Cour européenne des droits de l'homme (CEDH) a construit une jurisprudence en la matière. La Cour juge que « *la protection des données à caractère personnel joue un rôle fondamental pour l'exercice du droit*

89. Décision n° 2004/535/CE de la Commission du 14 mai 2004 relative au niveau de protection adéquat des données à caractère personnel contenues dans les dossiers des passagers aériens transférés au Bureau des douanes et de la protection des frontières des États-Unis d'Amérique.

90. CJCE, Gde Ch., 30 mai 2006, *Parlement européen c/ Conseil et Commission*, C-317/04 et 318/04.

91. G. Braibant, *La charte des droits fondamentaux de l'Union européenne : témoignages et commentaires*, p. 112, Paris, ed. Seuil, 2001.

au respect de la vie privée et familiale consacré par l'article 8 de la Convention » (CEDH, Gde Ch., 4 décembre 2008, *S. et Marper c. Royaume-Uni*, n° 30562/04 et 305566/04). Interprétant l'article 8 à la lumière de la convention n° 108 sur la protection des données et de recommandations du Comité des ministres du Conseil de l'Europe, elle considère que le droit interne de chaque État doit assurer que ces données sont pertinentes et non excessives par rapport aux finalités pour lesquelles elles sont enregistrées et qu'elles sont conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire aux finalités pour lesquelles elles sont enregistrées.

La CEDH a notamment eu à se prononcer sur les atteintes que les États peuvent porter à la vie privée pour des raisons de sécurité. Le texte de la convention lui-même admet que des atteintes puissent être portées en raison de certaines finalités : l'article 8.2 stipule qu'il « *ne peut y avoir ingérence d'une autorité publique dans l'exercice de ce droit que pour autant que cette ingérence est prévue par la loi et qu'elle constitue une mesure qui, dans une société démocratique, est nécessaire à la sécurité nationale, à la sûreté publique, au bien-être économique du pays, à la défense de l'ordre et à la prévention des infractions pénales, à la protection de la santé ou de la morale, ou à la protection des droits et libertés d'autrui* ». Dans une affaire *Leander c. Suède* (CEDH, 26 mars 1987, n° 9248/81), la Cour a jugé que « *le simple fait de mémoriser des données relatives à la vie privée d'un individu constitue une ingérence au sens de l'article 8* ». Elle a toutefois admis l'existence d'un registre secret de la police, pouvant être consulté pour le recrutement à des postes sensibles pour la sécurité nationale : elle juge que « *pour préserver la sécurité nationale, les États contractants ont indéniablement besoin de lois qui habilitent les autorités internes compétentes à recueillir et à mémoriser dans des fichiers secrets des renseignements sur des personnes, puis à les utiliser quand il s'agit d'évaluer l'aptitude de candidats à des postes importants du point de vue de ladite sécurité* » ; un tel système peut donc être admis sous réserve de « *l'existence de garanties adéquates et suffisantes contre les abus* ». En revanche, elle a estimé contraire à l'article 8 une législation permettant la conservation pendant une durée indéterminée d'empreintes digitales, d'échantillons biologiques et de profils ADN de personnes soupçonnées d'avoir commis une infraction mais non condamnées, dès lors qu'elle « *ne traduit pas un juste équilibre entre les intérêts publics et privés concurrents en jeu* » et « *ne peut passer pour nécessaire dans une société démocratique* » (arrêt *S. et Marper c. Royaume-Uni* précité).

• *Le droit à la protection des données personnelles dans la jurisprudence constitutionnelle*

La reconnaissance du droit à la protection des données personnelles par la jurisprudence constitutionnelle n'a été que progressive et récente. Dans son rapport de 1998, Guy Braibant relevait que le Conseil constitutionnel s'était refusé à tirer de la loi du 6 janvier 1978 un principe fondamental reconnu par les lois de la République. Le Conseil constitutionnel s'est d'abord fondé sur le droit à la vie privée, qu'il déduit de la liberté garantie par l'article 2 de la Déclaration des droits de l'homme et du citoyen. Après avoir jugé que « *la méconnaissance du droit au respect de la vie privée peut être de nature à porter atteinte à la liberté*

individuelle » (décision n° 94-352 DC du 18 janvier 1995, *Loi d'orientation et de programmation relative à la sécurité*, §3), il affirme plus nettement que « *la liberté proclamée par [l'article 2 de la Déclaration] implique le respect de la vie privée* » (décision n° 99-416 DC du 23 juillet 1999, *Loi portant création d'une couverture maladie universelle*, §45). Ce n'est qu'en 2012 que le Conseil constitutionnel a précisé les implications du droit à la vie privée en matière de protection des données personnelles : il juge que « *la collecte, l'enregistrement, la conservation, la consultation et la communication de données à caractère personnel doivent être justifiés par un motif d'intérêt général et mis en œuvre de manière adéquate et proportionnée à cet objectif* » (décision n° 2012-652 DC du 22 mars 2012, *Loi relative à la protection de l'identité*, §8).

Le Conseil constitutionnel exerce son contrôle sur les textes législatifs instaurant un traitement de données. Il s'assure de la proportionnalité des données collectées à la finalité d'intérêt général poursuivie ; selon un commentaire autorisé, ce contrôle est plus strict lorsque n'est pas en cause un fichier de police ou de justice, car « *l'objectif de recherche des auteurs d'infraction n'est en effet plus invocable* »[92]. Il veille à la présence de garanties appropriées, telles que l'application des garanties générales de la loi du 6 janvier 1978, la définition suffisamment précise des finalités du fichier dans la loi, la délimitation précise des personnes pouvant accéder aux fichiers, le cas échéant par une procédure d'habilitation, l'application du secret professionnel à ces personnes ou encore l'existence de sanctions pénales punissant le non-respect des règles d'utilisation du fichier. À l'inverse, l'imprécision de la loi sur les finalités et les conditions d'utilisation du traitement de données ou sur la nature des données collectées et sur les garanties assurant leur intégrité et leur confidentialité a pu être à l'origine de décisions d'annulation.

Sélection de décisions du Conseil constitutionnel sur des lois instaurant des traitements de données à caractère personnel

Les fichiers de police judiciaire : Le Conseil constitutionnel a jugé conformes à la Constitution les dispositions de la loi sur la sécurité intérieure relatives aux traitements automatisés de données nominatives mis en œuvre par les services de la police nationale et de la gendarmerie nationale dans le cadre de leurs missions (décision n° 2003-467 DC du 13 mars 2003, *Loi sur la sécurité intérieure*, §17 à 46). Rappelant qu'il appartient au législateur « *d'assurer la conciliation entre, d'une part, la sauvegarde de l'ordre public et la recherche des auteurs d'infractions, toutes deux nécessaires à la protection de principes et de droits de valeur constitutionnelle et, d'autre part, le respect de la vie privée et des autres droits et libertés constitutionnellement protégés* », le Conseil constitutionnel a considéré que le texte apportait des garanties suffisantes, notamment le contrôle du procureur de la République, le principe d'effacement en cas de décision de relaxe ou d'acquittement devenue définitive et la limitation des personnes habilitées à utiliser les traitements au titre de leurs attributions de police judiciaire. S'agissant de la consultation à des fins

92. Commentaire de la décision n° 2012-652 DC du 22 mars 2012, p. 14, http://www.conseil-constitutionnel.fr/conseil-constitutionnel/root/bank/download/2012652DCccc_652dc.pdf.

administratives de données recueillies dans le cadre d'activités de police judiciaire, il a jugé qu'elle pouvait être admise en raison de sa limitation à des fins déterminées (recrutement pour l'accès à certains emplois, instruction des demandes d'acquisition de la nationalité française et de renouvellement des titres de séjour, mesures de protection ou de défense prises dans les secteurs de sécurité des installations prioritaires de défense). Le Conseil a confirmé la constitutionnalité de ces dispositions à l'occasion de leur codification dans le code de procédure pénale (décision n° 2011-625 DC du 10 mars 2011, *Loi d'orientation et de programmation pour la performance de la sécurité intérieure*, §9 à 13).

Le fichier national automatisé des empreintes génétiques (FNAEG) : Le FNAEG a été créé par la loi n° 98-468 du 17 juin 1998 relative à la prévention et à la répression des infractions sexuelles ainsi qu'à la protection des mineurs. Son objet, au départ réservé à la recherche et à l'identification des auteurs d'infractions sexuelles, a été progressivement élargi à bien d'autres crimes et délits, tels que les atteintes volontaires à la vie de la personne, le trafic de stupéfiants, le proxénétisme ou les actes de terrorisme. Saisi d'une question prioritaire de constitutionnalité, le Conseil constitutionnel a jugé conformes à la Constitution les dispositions du code de procédure pénale relatives au FNAEG (décision n° 2010-25 QPC du 16 septembre 2010). Il s'est fondé sur l'ensemble des garanties entourant la mise en œuvre du fichier, notamment le contrôle de la CNIL, celui d'un magistrat, le fait qu'il ne concerne que les personnes condamnées pour certaines infractions et celles pour lesquelles il existe des indices graves et concordants, ou encore l'existence du droit d'accès prévu par l'article 39 de la loi du 6 janvier 1978. Il a également relevé que les empreintes génétiques conservées permettaient seulement l'identification des personnes et non la recherche de leurs caractéristiques génétiques.

Le fichier central des titres d'identité et la « puce e-Service » : Une proposition de loi avait été votée par le Parlement pour créer un fichier central des titres d'identité, comportant pour chaque Français des données biométriques (les empreintes digitales), dans le but de lutter contre la fraude documentaire. Le Conseil constitutionnel a jugé que ce dispositif n'était pas conforme à la Constitution (décision n° 2012-652 DC du 22 mars 2012, *Loi relative à la protection de l'identité*). Il a estimé que la lutte contre la fraude était une finalité d'intérêt général, mais que le traitement prévu par la loi portait une atteinte disproportionnée au but poursuivi, en raison de l'ampleur du traitement (qui devait couvrir la quasi-totalité de la population française), de la nature des données enregistrées (données biométriques, que le Conseil constitutionnel qualifie de « *particulièrement sensibles* » car elles sont « *susceptibles d'être rapprochées de traces physiques laissées involontairement par la personne ou collectées à son insu* ») et de ses caractéristiques techniques et des conditions de sa consultation (le fichier peut être consulté à d'autres fins que la vérification de l'identité d'une personne lors de la délivrance ou du renouvellement d'un titre d'identité).

La loi prévoyait également que la carte d'identité pourrait contenir, si son titulaire le souhaite, un composant, qualifié de « puce eService », permettant de s'identifier sur les réseaux numériques et d'apposer sa signature électronique. Le Conseil constitutionnel a censuré cette disposition pour incompétence négative du législateur. Il a jugé « *qu'en l'état actuel des moyens de communication et eu égard au développement généralisé des services de communication au public en ligne ainsi qu'à l'importance prise par ces services dans la vie économique et sociale, les conditions générales dans lesquelles la carte nationale d'identité délivrée par l'État peut permettre à une personne de s'identifier sur les réseaux de communication électronique et de mettre en œuvre sa signature électronique, notamment à des fins civiles et commerciales, affectent directement les règles et les principes précités et, par suite, relèvent du domaine de la loi* » et que la loi qui lui était soumise ne précisait ni la nature des données utilisées, ni les conditions dans lesquelles l'authentification était mise en œuvre, notamment pour une personne mineure ou faisant l'objet d'une mesure de protection juridique.

Le registre national des crédits aux particuliers : Une loi relative à la consommation créait un registre national recensant les crédits à la consommation accordés aux personnes physiques, créant ainsi ce qui est parfois qualifié de « fichier positif »[93]. Le Conseil constitutionnel a estimé que si la prévention des situations de surendettement constitue un motif d'intérêt général, l'atteinte portée au droit à la vie privée était disproportionnée, « *eu égard à la nature des données enregistrées, à l'ampleur du traitement, à la fréquence de son utilisation, au grand nombre de personnes susceptibles d'y avoir accès et à l'insuffisance des garanties relatives à l'accès au registre* » (décision n° 2014-690 DC du 13 mars 2014, § 57).

• *Un corpus juridique cohérent*

En dépit de la multiplicité des normes intervenant dans la protection des données personnelles, une grande convergence se dessine sur les principales garanties de cette protection, qu'on peut énumérer ainsi :

- principes relatifs à la qualité des données (loyauté de la collecte, finalités déterminées et légitimes, proportionnalité des données collectées et de leur durée de conservation aux finalités, exactitude) ;

- exigence du consentement de la personne concernée ou d'un autre fondement légitime prévue par la loi ;

- interdiction de la collecte de certaines données sensibles (opinion religieuse ou politique, origine ethnique, santé, orientation sexuelle), sauf dans des cas particuliers prévus par la loi ;

- droits d'information, d'accès, de rectification et d'opposition de la personne concernée ;

93. Par opposition au « fichier négatif » que constitue le fichier des incidents de remboursement des crédits en particuliers (FICP), qui ne recense que les incidents, le fichier positif aurait recensé tous les crédits.

- obligation de sécurité du responsable du traitement ;

- existence d'une autorité indépendante de contrôle chargée de veiller à la mise en œuvre de ces dispositions.

La décision du Conseil d'État *Association pour la promotion de l'image* (CE, Ass., 26 octobre 2011, n° 317827, Rec. p. 505) illustre la convergence des différentes normes existant en matière de protection des données personnelles. Saisi d'un recours contre un décret relatif aux passeports biométriques, le Conseil d'État énumère les différentes normes au regard desquelles il exerce son contrôle (Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales, Convention internationale des droits de l'enfant, loi du 6 janvier 1978) et en déduit des principes communs, définis dans un considérant unique : « *Considérant qu'il résulte de l'ensemble de ces dispositions que l'ingérence dans l'exercice du droit de toute personne au respect de sa vie privée que constituent la collecte, la conservation et le traitement, par une autorité publique, d'informations personnelles nominatives, ne peut être légalement autorisée que si elle répond à des finalités légitimes et que le choix, la collecte et le traitement des données sont effectués de manière adéquate et proportionnée au regard de ces finalités* ».

Un cadre qui s'est adapté à l'essor du numérique

Le citoyen ou l'entreprise qui cherche dans la loi du 6 janvier 1978 les règles applicables à ses usages numériques peut être dérouté. Nulle part il n'y est question de moteurs de recherche, de réseaux sociaux ou de géolocalisation ; même le terme « *internet* » n'y apparaît pas. Les interrogations sur la pertinence de ce cadre juridique au regard du bouleversement des technologies et des usages du numérique, tel qu'il a été présenté ci-dessus (cf. 1.1), sont donc naturelles.

Il est cependant manifeste que c'est justement en raison de la généralité de ses termes et des notions juridiques employées (généralité qu'elle partage d'ailleurs avec la convention n° 108 du Conseil de l'Europe et la directive du 24 octobre 1995) que la loi du 6 janvier 1978 a pu continuer à s'appliquer jusqu'à aujourd'hui. Si la loi avait employé des termes correspondant aux développements de l'informatique de son époque, tels que ceux de bande magnétique, de bi-processeurs ou de mini-ordinateurs, elle aurait très vite été datée. Grâce à ce choix, la loi du 6 janvier 1978 a pu faire exception à l'instabilité législative. Elle n'a connu qu'une réforme d'ampleur, opérée par la loi du 6 août 2004 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel, ainsi que quelques modifications ponctuelles (création de dispositions propres à certains traitements de données de santé par deux lois du 1er juillet 1994 et du 27 juillet 1999 ; obligation d'information des personnes concernées par les fournisseurs de services de communications électroniques en cas de violation de données personnelles, créée par une ordonnance du 24 août 2011).

Stable, le cadre issu de la loi du 6 janvier 1978 n'est pas pour autant demeuré immobile. Deux éléments ont contribué à son adaptation à l'essor du numérique : l'importante réforme opérée par la loi du 6 août 2004 ; l'application des concepts généraux de la loi aux situations particulières, qui résulte de la jurisprudence et d'instruments de droit souple.

La loi du 6 août 2004 est intervenue pour transposer la directive du 24 octobre 1995. Si l'informatique avait beaucoup évolué entre 1978 et 1995, avec notamment la généralisation de l'informatique personnelle, internet n'en était encore qu'à ses premiers pas ; entre l'adoption de la directive et sa transposition en France, il était entré dans les mœurs. La loi du 6 août 2004 est donc elle aussi datée. Elle a cependant permis de mettre à jour la loi du 6 janvier 1978, notamment en déplaçant sa focalisation des traitements de données du secteur public vers ceux du secteur privé. La loi originelle soumettait les traitements du secteur public à un régime d'autorisation et ceux du secteur privé à un régime de déclaration. La loi du 6 août 2004 abandonne cette distinction, qui n'était pas retenue par la directive : le régime de déclaration devient le droit commun, pour le secteur public comme pour le secteur privé ; certaines catégories de traitement définies par les articles 25 à 27 en fonction de leur sensibilité doivent être autorisées par la CNIL ou par un arrêté ministériel ou un décret en Conseil d'État pris après avis de la CNIL. Il s'agit notamment des traitements portant sur l'une des données sensibles énumérées par l'article 8, des traitements comportant des données biométriques, des traitements utilisant le numéro d'inscription au répertoire (NIR), des traitements comportant des appréciations sur les difficultés sociales des personnes ou encore des traitements assurant l'interconnexion de fichiers poursuivant des finalités différentes. Ce changement du cadre législatif a permis une profonde réorientation de l'activité de la CNIL : déchargée de l'obligation d'examiner le moindre traitement de données du secteur public, elle consacre aujourd'hui la majeure partie de son activité à contrôler des traitements de données du secteur privé. Ainsi, en 2012, seules 8 % des plaintes soumises à la CNIL entraient dans la rubrique « libertés publiques-collectivités » ; les secteurs « internet/télécoms », « commerce », « travail » et « banques » totalisaient à eux quatre 77 % des plaintes[94]. Ce basculement était sans nul doute nécessaire, compte tenu de l'extension considérable des traitements de données effectués par les personnes privées et de leurs enjeux pour la protection des données personnelles (cf. *supra* 1.1). Pour autant, certains traitements sensibles propres à la puissance publique demeurent soumis au régime d'autorisation : il s'agit notamment des traitements intervenant dans les matières régaliennes, telles que la sécurité publique ou la justice pénale, ainsi que des traitements mis en œuvre par les organismes de sécurité sociale, en raison de leur utilisation du NIR.

D'autres adaptations à l'essor du numérique résultent de la loi du 6 août 2004. Les flux de données vers les États, très limités en 1978, font désormais l'objet du chapitre XII de la loi. Des dispositions spécifiques encadrent l'utilisation des données biométriques et des données génétiques. En termes de vocabulaire, la loi du 6 août 2004 substitue aux termes « *d'informations nominatives* » ceux de « *données à caractère personnel* ».

En dehors de ces quelques modifications du texte législatif, c'est à la jurisprudence et au droit souple qu'il est revenu d'appliquer les notions générales de données à caractère personnel, de traitement de données, de finalités déterminées ou encore de consentement, aux évolutions des usages du numérique. La qualification

94. CNIL, *Rapport d'activité 2012*, p. 46, avril 2013.

juridique des faits, tels qu'ils ressortent des affaires qui lui sont soumises, au regard des textes qu'il applique, relève de la mission habituelle du juge. Quant au droit souple, il a été défini par une précédente étude du Conseil d'État comme l'ensemble des instruments non contraignants ayant pour objet de modifier les comportements de leurs destinataires, et qui présentent une structuration et une formalisation les apparentant à des règles de droit[95]. C'est par des instruments de droit souple, tels que des avis, des recommandations ou des lignes directrices, que la CNIL et le G29 ont indiqué comment ils interprétaient les concepts de la loi du 6 janvier 1978 et de la directive du 24 octobre 1995 à la lumière des nouveaux usages du numérique. Trois sujets peuvent illustrer ce rôle de la jurisprudence et du droit souple : les moteurs de recherche, les réseaux sociaux et la géolocalisation.

Les moteurs de recherche, qui sont des outils incontournables dans l'accès à l'information contenue sur internet, ont rapidement attiré l'attention des autorités de protection des données. Une première résolution sur les enjeux de protection de la vie privée liés aux moteurs de recherche a été adoptée par un groupe de travail de la Conférence internationale des autorités de protection des données[96] dès le 15 avril 1998. L'avis adopté par le G29 le 9 avril 2008[97] recense les enjeux de données personnelles liés aux moteurs de recherche : d'une part, les moteurs de recherche traitent directement des données personnelles, à travers des fichiers « *logs* »[98], le recueil de l'adresse IP et l'enregistrement de « *cookies* » sur le terminal de l'utilisateur ; d'autre part, les moteurs de recherche sont des outils puissants pour regrouper les informations sur une personne disséminées sur le *web*. Le G29 qualifie les éditeurs de moteurs de recherche de responsables de traitement au sens de la directive du 24 octobre de 1995, en ce qui concerne les données personnelles qu'ils traitent directement ; en revanche, s'agissant des sites auxquels renvoie le moteur de recherche, qui peuvent contenir des données personnelles, le G29 considère que les moteurs de recherche n'en sont pas responsables, dans la mesure (et dans cette mesure seulement) où ils agissent comme des intermédiaires techniques neutres. Il analyse enfin, au regard des différents fondements possibles prévus par l'article 7 de la directive (consentement, exécution d'un contrat, intérêt légitime du responsable du traitement) la licéité des pratiques des moteurs de recherche. L'avis pointe en particulier le caractère insuffisamment précis des finalités indiquées par les moteurs de recherche pour justifier leur collecte de données personnelles, telles que « *l'amélioration du service rendu aux utilisateurs* », qui poserait problème au regard de l'exigence formulée par l'article 6 de finalités « *déterminées, explicites et légitimes* ». C'est dans le prolongement de cet avis que les autorités européennes

95. Conseil d'État, *Le droit souple*, La documentation Française, 2013.

96. L'*International Conference of Data Protection and Privacy Commissioners* a été créée en 1979 et rassemble des autorités de protection des données du monde entier ; en dehors de l'Europe, elle compte notamment les autorités du Canada, de l'Australie, de la Nouvelle-Zélande, du Mexique et de l'Uruguay, ainsi que la Federal Trade Commission pour les États-Unis. Elle se réunit une fois par an.

97. *Opinion 1/2008 on data protection issues related to search engines*, 00737EN/WP 148.

98. Ces fichiers recensant les requêtes formulées par un utilisateur et les liens sur lesquels ils ont cliqué.

de protection des données ont initié à l'encontre de *Google* une procédure coordonnée d'investigation sur la conformité de ses pratiques à la directive, qui a ensuite débouché sur l'adoption de sanctions par plusieurs autorités, notamment en France[99] et en Espagne. Si le débat contentieux est encore pendant devant les juridictions compétentes, la mise en œuvre de ces procédures de sanction témoigne de la possibilité d'appliquer les concepts généraux issus de la directive aux pratiques contemporaines des moteurs de recherche.

Le G29 a également rendu publique sa doctrine concernant les réseaux sociaux, par un avis du 12 juin 2009[100]. Il qualifie les réseaux sociaux de responsables de traitement de données à caractère personnel, tant en raison de leur utilisation des données pour faire fonctionner le service du réseau social que de leur mise à disposition à des fins publicitaires. Les fournisseurs tiers d'applications utilisables sur le réseau social reçoivent la même qualification. Le G29 souligne que les réseaux sociaux devraient proposer à leurs utilisateurs des réglages par défaut favorables à la vie privée (« *privacy-friendly* »). Il estime également qu'ils devraient informer les utilisateurs qu'ils ne peuvent poster sur le réseau des photos ou des informations sur des tiers sans leur consentement. Le G29 parvient donc à déduire des dispositions de la directive du 24 octobre 1995 des prescriptions détaillées à l'égard des éditeurs de réseaux sociaux.

Le développement des terminaux mobiles et l'accessibilité universelle du système GPS ont ouvert la voie à un nombre considérable d'applications, tant pour les acteurs privés que pour les pouvoirs publics en matière de police et de justice (sur ce dernier point, cf. *infra* 1.3.1). La CNIL a émis plusieurs recommandations au sujet de la géolocalisation des véhicules, concernant sa mise en œuvre d'une part par les compagnies d'assurances et les constructeurs automobiles, d'autre part par les employeurs à l'égard de leurs employés[101]. Dans ce dernier cas, la CNIL estime que « *les traitements de géolocalisation, en ce qu'ils permettent de localiser l'employé utilisant le véhicule au moment où s'effectue l'opération de géolocalisation, portent sur des données à caractère personnel et sont soumis aux dispositions de la loi du 6 janvier 1978 modifiée* ». Elle rappelle les obligations de poursuivre des finalités déterminées, explicites et légitimes ainsi que de ne pas exercer une surveillance disproportionnée. Elle estime que seules quatre finalités peuvent justifier la mise en œuvre de tels dispositifs : sécurité de l'employé ou des marchandises transportées, allocation des moyens pour des prestations à accomplir en des lieux dispersés, facturation d'une prestation de services liée à l'utilisation du véhicule ou mesure du temps de travail lorsqu'il n'existe pas d'autre possibilité moins intrusive. Elle considère qu'une durée de conservation des données de deux mois est proportionnée. Dans un esprit voisin, la Cour de cassation[102] a jugé que le licenciement d'un salarié fondé sur l'utilisation de données de géolocalisation était illicite, au motif « *qu'un système de géolocalisation ne peut être utilisé par*

99. Délibération n° 2013-420 du 3 janvier 2014 de la CNIL.

100. *Opinion 5/2009 on online social networking*, 01189/09/EN WP 163.

101. Il s'agit respectivement des délibérations n° 2010-096 du 8 avril 2010 et n° 2006-066 du 16 mars 2006.

102. Soc., 3/11/2011, n° 10-18.036.

l'employeur pour d'autres finalités que celles qui ont été déclarées auprès de la Commission nationale de l'informatique et des libertés, et portées à la connaissance des salariés », ce qui n'avait pas été le cas en l'espèce.

Ces exemples illustrent la possibilité d'appliquer les notions générales de la loi du 6 janvier 1978 et de la directive du 24 octobre 1995 aux phénomènes contemporains du numérique, montrant que ce cadre juridique a su s'adapter. Toutefois, malgré cet apport de la jurisprudence et du droit souple, des difficultés significatives se présentent, tant sur l'application de ce cadre à des acteurs extra- européens (cf. *infra* 1.4) que sur sa capacité à faire face aux risques les plus importants pour la protection des données personnelles (cf. *infra* 2.2). La proposition de règlement européen sur la protection des données, en date du 25 janvier 2012, vise à remédier à ces difficultés en se substituant à la directive. L'examen de ces difficultés et de la mesure dans laquelle la proposition de règlement y répond fera l'objet de la deuxième partie de cette étude.

1.2.2. Un nouveau droit fondamental de l'accès à internet

L'accès à internet a été reconnu, en France et dans d'autres pays, comme une condition de la liberté de communication ; il favorise également l'exercice d'autres droits fondamentaux, notamment la liberté d'entreprendre et la liberté d'association, ce qui amène à le considérer comme un droit fondamental à part entière. De ce droit découle le débat sur la neutralité du *net*, principe qui tend à garantir l'égal traitement de tous les utilisateurs d'internet.

Le droit d'accès à internet, un nouveau droit fondamental

La Cour suprême des États-Unis a été la première juridiction souveraine à être saisie des enjeux d'internet pour la liberté d'expression. Dans un arrêt *Reno, Attorney general of the United States vs American Civil Liberties Union (ACLU)* du 26 juin 1997, elle a jugé que des dispositions du *Communications Decency Act* de 1996, qui sanctionnaient pénalement la diffusion sur internet à des mineurs de contenus à caractère sexuel, étaient contraires au premier amendement de la Constitution garantissant la liberté d'expression. Elle a considéré que ces dispositions présentaient un caractère général et absolu et qu'elles conduisaient à supprimer massivement des contenus que des adultes avaient constitutionnellement le droit d'émettre et de lire. À cette occasion, elle a jugé que les restrictions à la liberté d'expression qu'elle avait admises dans des précédents concernant la diffusion audiovisuelle, en raison de la rareté des fréquences et du caractère « *intrusif* » de ce *medium*, n'étaient pas transposables à internet ; selon ses termes, internet doit recevoir, à la différence de l'audiovisuel, une « *protection complète au titre du premier amendement* ». C'est dans le cadre de cette affaire qu'a été formulée la phrase restée fameuse selon laquelle internet peut être regardé comme « *une conversation mondiale sans fin* »[103] ; elle émane de Stuart Dalzell, juge du tribunal de district dont le jugement était contesté devant la Cour suprême.

103. "*The Internet may fairly be regarded as a never-ending worldwide conversation*".

En France, le Conseil constitutionnel s'est prononcé à l'occasion d'un recours contre la loi favorisant la diffusion et la protection de la création sur internet. Cette loi confiait à une autorité administrative indépendante, la Haute Autorité pour la diffusion des œuvres et la protection des droits sur internet (HADOPI), le pouvoir de prononcer une sanction administrative de suspension de l'accès à internet à l'encontre d'une personne n'ayant pas veillé à ce que cet accès ne soit pas utilisé pour diffuser ou recevoir des contenus en méconnaissance des droits d'auteur. Le Conseil constitutionnel a jugé « *qu'en l'état actuel des moyens de communication et eu égard au développement généralisé des services de communication au public en ligne ainsi qu'à l'importance prise par ces services pour la participation à la vie démocratique et l'expression des idées et des opinions* », la liberté de communication protégée par l'article 11 de la Déclaration des droits de l'homme et du citoyen « *implique la liberté d'accéder à ces services* » (décision n° 2009-580 DC du 10 juin 2009, §12). La sanction de suspension de l'accès à internet pouvant « *conduire à restreindre l'exercice, par toute personne, de son droit de s'exprimer et de communiquer librement, notamment depuis son domicile* », il en a déduit que seule l'autorité judiciaire pouvait prononcer une telle peine.

Dans un sens voisin, la directive 2009/140/CE du Parlement européen et du Conseil du 25 novembre 2009, composante du « *troisième paquet télécoms* », dispose que « *les mesures prises par les États membres concernant l'accès des utilisateurs finals aux services et applications, et leur utilisation, via les réseaux de communications électroniques respectent les libertés et droits fondamentaux des personnes physiques, tels qu'ils sont garantis par la Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales et les principes généraux du droit communautaire* » ; elle impose le respect de la présomption d'innocence et la mise en place d'une procédure « *préalable, équitable et impartiale* » avant toute restriction de l'accès. La professeure Laure Marino souligne la parenté et la contemporanéité entre la décision du Conseil constitutionnel et les discussions préparatoires à l'adoption de la directive. Le Parlement européen était allé jusqu'à adopter, lors d'un vote le 6 mai 2009, « *le principe selon lequel aucune restriction ne peut être imposée aux droits et libertés fondamentaux des utilisateurs finaux sans décision préalable des autorités judiciaires* » ; le texte final ne va pas jusqu'à imposer l'intervention préalable de l'autorité judiciaire, mais reprend bien l'idée que l'accès à internet est un droit fondamental.

De même qu'il rattache le droit à la protection des données personnelles au droit à la vie privée, le Conseil constitutionnel inclut l'accès à internet dans la liberté de communication. Toutefois, et comme pour le droit à la protection des données personnelles, on peut considérer que l'accès à internet concourt à garantir bien d'autres droits. Selon la formule du rapporteur spécial des Nations unies sur la promotion et la protection du droit à la liberté d'opinion et d'expression, M. Frank La Rue, l'accès à internet est « *aussi bien un droit fondamental en lui-même qu'un « facilitateur » d'autres droits, comportant les droits économiques, sociaux et culturels, tels que le droit à l'éducation, le droit de prendre part à la vie culturelle et de jouir du progrès scientifique et de ses applications, ainsi que les droits civils et politiques, tels que les droits d'association et de réunion* »[104].

104. F. La Rue, *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression*, Nations Unies, mai 2011.

Le Conseil constitutionnel a reconnu une obligation négative incombant à l'État, celle de ne pas couper l'accès à internet. Le débat se prolonge aujourd'hui sur l'existence d'obligations positives des pouvoirs publics à l'égard de catégories de personnes qui en sont dépourvues, en raison d'une privation de liberté, d'une incapacité physique ou d'un manque de moyens matériels.

La question de l'accès à internet des prisonniers fait aujourd'hui l'objet d'un recours pendant devant la CEDH, de la part d'une personne qui l'avait demandé en vue de s'inscrire au cours d'une université (*Jankovskis c/ Lituanie*, n° 21575/08). En France, le Contrôleur général des lieux de privation de liberté a préconisé d'ouvrir aux prisonniers un accès contrôlé à internet, dans son rapport d'activité 2013 comme dans de précédents rapports. Il soutient notamment que l'accès à internet est utile pour la préparation de la réinsertion.

S'agissant des personnes affectées d'une incapacité, la convention des Nations unies du 13 décembre 2006 relative aux droits des personnes handicapées stipule en son article 9 que les États doivent assurer l'accès à « *l'information et à la communication, y compris aux systèmes et technologies de l'information et de la communication* ». Une proposition de la directive de l'Union européenne relative à l'accessibilité des sites *web* d'organismes du secteur public, en date du 3 décembre 2012[105], prévoit d'imposer aux États membres de prendre d'ici le 31 décembre 2015 les mesures nécessaires pour faire en sorte que les sites *web* concernés soient accessibles. La directive renvoie à des « *normes harmonisées* » la définition des prescriptions techniques détaillées à respecter ; les sites qui les appliqueront bénéficieront d'une présomption de conformité à la directive.

L'absence d'accès à internet risque à l'avenir d'être un facteur d'exclusion d'autant plus fort qu'une majorité de plus en plus large de la population est connectée, conduisant à ce qu'un nombre croissant d'activités économiques et sociales ou de formalités administratives passent par ce *medium*. En 2013, le taux d'équipement en connexion à internet à domicile atteint 81 % pour l'ensemble de la population française, mais il n'est que de 58 % pour les personnes dont les revenus sont inférieurs à 900 euros par mois[106]. Dans un rapport sur « *l'inclusion numérique* », le Conseil national du numérique préconise une gamme de mesures, notamment le développement de tarifs sociaux ciblés pour l'internet et le mobile ainsi que des « *espaces publics numériques* »[107]. Cependant, la directive n° 2002/22/CE du 7 mars 2002, dite « *directive service universel* », ne permet pas d'inclure la fourniture de tels tarifs sociaux couvrant l'accès à internet dans les obligations de service universel financées par la contribution des opérateurs[108] ; ils peuvent donc seulement être aujourd'hui proposés de manière volontaire par les opérateurs.

---

105. 2012/0340 (COD).

106. CREDOC, Enquête « Conditions de vie et Aspirations», juin 2013.

107. Conseil national du numérique, *Citoyens d'une société numérique*, novembre 2013.

108. Cf. Autorité de la concurrence, avis n° 11-A-10 du 29 juin 2011 portant sur la mise en place d'un tarif social permettant l'accès des personnes aux revenus modestes aux services Internet haut débit.

Le principe de neutralité du net *fait l'objet de débats sur son contenu et la place à lui reconnaître dans le droit positif*

Le concept de « *neutralité du* net » (« *network neutrality* ») a été formulé pour la première fois par le juriste américain Tim Wu, dans un article de 2003[109], écrit dans le contexte du débat suscité aux États-Unis par les pratiques d'opérateurs de télécommunications, qui entravaient l'accès de leurs abonnés à certains services ou à certaines applications. La neutralité du *net* implique que tous les opérateurs, qu'il s'agisse des fournisseurs d'accès à internet (FAI) en contact avec les utilisateurs finaux ou de ceux assurant l'interconnexion entre les réseaux, traitent de manière égale tous les flux de données quel que soit leur contenu : selon la formulation donnée par Tim Wu, « *un réseau public d'utilité maximale aspire à traiter tous les contenus, sites et plateformes de la même manière, ce qui lui permet de transporter toute forme d'information et d'accepter toutes les applications* »[110]. La neutralité correspond à l'architecture originelle d'internet, qui repose sur le principe du « meilleur effort » (« *best effort* ») : chaque opérateur fait de son mieux pour assurer la transmission de tous les paquets de données qui transitent par son réseau, sans garantie de résultat et sans discrimination. Selon les partisans de la neutralité du *net*, elle a été déterminante pour favoriser la croissance d'internet et le développement de nouveaux services : grâce à elle, chaque innovateur a le même accès à ses clients potentiels. Elle a partie liée avec le droit d'accès à internet et la liberté d'expression : elle permet en effet à chacun d'émettre et de recevoir des contenus dans les mêmes conditions.

Une série de facteurs techniques, économiques et politiques conduisent cependant les opérateurs à différencier le traitement des paquets selon leur contenu. Les débats sur la neutralité du *net* ont pour objet de déterminer si ce principe doit être inscrit dans le droit positif afin de restreindre ces possibilités de différenciation et, si oui, lesquelles doivent être admises.

Sur le plan technique, les opérateurs sont conduits à mettre en place des pratiques dites de « gestion de trafic ». Celle-ci est définie par l'ARCEP comme recouvrant « *toutes les formes techniques d'intervention sur les flux de données mises en œuvre en prenant en compte la nature du trafic, ou encore l'identité ou la qualité de son émetteur ou de son destinataire* »[111]. Leur but peut être d'optimiser l'allocation des ressources de l'opérateur et la qualité de service ressentie par l'utilisateur, de prévenir la congestion du réseau ou de lutter contre les virus ou les *spams*. L'enjeu est également de diffuser les « services gérés » qui, à la différence de l'internet ordinaire fonctionnant selon le principe du meilleur effort, impliquent une garantie de qualité ; il s'agit notamment des services de téléphonie ou de télévision sur internet, qui se sont beaucoup développés en France dans les années 2000 avec

109. T. Wu, "Network Neutrality, Broadband Discrimination", *Journal of Telecommunications and High Technology Law*, Vol. 2, p. 141, 2003.

110. Traduction donnée par l'ARCEP, *Neutralité de l'internet et des réseaux. Propositions et recommandations,* septembre 2010.

111. Ibid, p. 10.

les offres dites « *triple play* ». Les « services gérés » transitent par les mêmes réseaux que le trafic ordinaire, ce qui implique donc de la part des opérateurs une réservation prioritaire de capacité à leur profit.

Sur le plan économique, le débat sur la neutralité du *net* est lié à la question du mode de rémunération des opérateurs. En effet, ceux-ci ne sont rémunérés que par les utilisateurs finaux et non par les fournisseurs de contenus. Face aux capacités croissantes requises par le développement du trafic vidéo et au coût des investissements dans les infrastructures du très haut débit (fibre optique pour l'internet fixe, 4G et à moyen terme 5G pour l'internet mobile[112]), les opérateurs demandent souvent à faire payer les fournisseurs de contenus, du moins ceux qui génèrent le trafic le plus important[113]. Ce paiement conduirait alors à leur réserver en contrepartie des capacités prioritaires, de manière à leur garantir une qualité de diffusion supérieure. Une autre difficulté tient à la tentation que peuvent avoir les fournisseurs d'accès à internet de dégrader ou de bloquer l'accès à des services concurrents de ceux qu'ils proposent ; par exemple, un fournisseur d'accès à internet qui est également un opérateur de téléphone peut avoir intérêt à dégrader l'accès à un service de « *voix sur IP* » comme *Skype*[114].

Sur le plan politique, les pouvoirs publics peuvent imposer aux opérateurs de bloquer ou au contraire de favoriser certains contenus. En France, des pouvoirs de blocage des sites à caractère pédopornographique ont été conférés à l'autorité administrative par la loi du 14 mars 2011 d'orientation et de programmation pour la performance de la sécurité intérieure (dite *LOPPSI 2*). La loi pour la confiance dans l'économie numérique avait même prévu un dispositif général de blocage administratif de sites, pour divers motifs (risque d'atteinte à l'ordre public, à la protection des mineurs, de la santé publique ou encore des consommateurs) dont le décret d'application n'a cependant jamais été pris et qui a été abrogé par la loi relative à la consommation du 17 mars 2014. En matière de lutte contre la contrefaçon, la loi du 12 juin 2009 favorisant la diffusion et la protection de la création sur internet a donné au juge judiciaire le pouvoir d'ordonner « *toutes mesures propres à prévenir ou à faire cesser une (…) atteinte à un droit d'auteur ou un droit voisin, à l'encontre de toute personne susceptible de contribuer à y remédier* »[115]. C'est sur ce fondement que dans un jugement du 28 novembre 2013, le tribunal de grande instance de Paris a enjoint à plusieurs fournisseurs d'accès (*Orange, Bouygues Télécom, Numericable,* etc.) de bloquer l'accès à des

112. Il est d'usage de classer les standards techniques de la téléphonie mobile en « générations ». La téléphonie mobile a pris son essor dans les années 1990 avec la « 2G », représentée en Europe par la norme GSM. La « 3G », correspondant en Europe à la norme UMTS, a été commercialisée à partir du milieu des années 2000 et a permis le développement de l'internet mobile. La « 4G », correspondant à la norme LTE, a commencé à être commercialisée à grande échelle en Europe en 2013 et est souvent qualifiée de « *très haut débit* ». Les standards de la « 5G » sont en cours de développement et devraient accélérer le déploiement des objets connectés.

113. Aux heures de pointe, *Netflix* et *Youtube* représenteraient 50 % du trafic aux États-Unis.

114. Cf. par ex. aux États-Unis la décision de 2005 de la *Federal Communications Commission* à l'encontre de l'opérateur *Madison River*, mettant en évidence ce type de pratiques.

115. Article L. 336-2 du code de la propriété intellectuelle.

sites tels que *Allostreaming*, proposant la lecture de vidéos en méconnaissance des droits d'auteur. S'il n'existe pas à ce jour de dispositif imposant aux opérateurs de communications électroniques de favoriser certains contenus répondant à des objectifs de politique publique, des propositions ont pu être faites en ce sens. Le rapport de Pierre Lescure et le Conseil supérieur de l'audiovisuel (CSA) ont ainsi préconisé que les fournisseurs de services culturels en ligne signant une convention avec le CSA, comportant des engagements d'exposition de la création européenne et française et de financement de la création, puissent bénéficier d'une priorité dans la gestion des débits, les avantageant dans l'accès aux consommateurs[116].

Le principe de neutralité du *net* fait l'objet de vives controverses aux États-Unis depuis le début des années 2000. Le 23 septembre 2005, l'agence américaine chargée de la supervision du secteur des télécommunications, la *Federal Communications Commission* (FCC), a défini dans un « *policy statement* » quatre principes tendant à garantir la neutralité du *net* : les consommateurs ont le droit d'accéder sur internet à tout contenu licite de leur choix ; les consommateurs ont le droit d'utiliser les applications et les services de leur choix, sous réserve des besoins de l'exécution des lois ; les consommateurs ont le droit de connecter à internet tout matériel qui ne porte pas atteinte au bon fonctionnement du réseau ; les consommateurs ont le droit de bénéficier de la concurrence entre les fournisseurs d'accès, de services, d'applications et de contenus. Cependant, plusieurs décisions de la FCC tendant à assurer la mise en œuvre de ces principes ont été annulées par la justice américaine, au motif que la FCC n'a pas l'autorité légale pour les imposer[117]. Le nouveau projet de réglementation soumis à la concertation publique par la FCC en mai 2014 est très critiqué, dans la mesure où il permet aux opérateurs de faire payer les fournisseurs de contenus pour maintenir une vitesse de connexion optimale. Par ailleurs, faute de consensus entre les démocrates, favorables à la reconnaissance de la neutralité du *net*, et les républicains, qui y sont opposés, aucune des propositions de loi tendant à consacrer ce principe n'a été votée par le Congrès. Les opposants à la neutralité du *net* soutiennent que des règles contraignantes risquent d'entraver l'innovation et les investissements dans le réseau, alors que le libre jeu du marché suffirait à prévenir les risques de discrimination ; la neutralité du *net* serait une « *solution à la recherche d'un problème* »[118].

En France, la neutralité du *net* a fait l'objet jusqu'à présent d'une démarche plus progressive des pouvoirs publics. L'ARCEP a formulé en 2010 dix recommandations non contraignantes. Les quatre premières, relatives aux principes dont l'ARCEP préconise le respect, sont les suivantes :

---

116. P. Lescure, *op. cit,* p. 153 ; CSA, *op. cit.*, p. 55.

117. La FCC a d'abord été désavouée dans un cas particulier par l'arrêt *Comcast Corp. v. FCC*, 6/4/2010, 600 F.3d 642 de la cour d'appel fédérale du district de Columbia. Dans l'arrêt *Verizon v. FCC*, 14/1/2014, n° 11-1355, la même cour a annulé la réglementation relative à la neutralité du *net* (*Open Internet Order*).

118. Cf. par ex. D. Brenner, "Net Neutrality: A Solution In Search Of A Problem", *Forbes*, 25 septembre 2012, http://www.forbes.com/sites/ciocentral/2012/09/25/net-neutrality-a-solution-in-search-of-a-problem/.

- la recommandation n° 1 préconise aux opérateurs de garantir les droits suivants de l'utilisateur final : liberté d'envoyer et de recevoir le contenu de son choix, possibilité d'utiliser les services ou de faire fonctionner les applications de son choix, possibilité de connecter le matériel et d'utiliser les programmes de son choix, dès lors qu'ils ne nuisent pas au réseau ;

- la recommandation n° 2 énonce un principe de non-différenciation des flux de données, auquel les opérateurs ne devraient déroger que dans le cadre prévu à la recommandation n° 3 ;

- selon la recommandation n° 3, les pratiques de gestion de trafic des opérateurs doivent respecter des critères de pertinence, de proportionnalité, d'efficacité, de non discrimination des acteurs et de transparence ;

- la recommandation n° 4 admet la possibilité pour les opérateurs de proposer des « *services gérés* », à condition que cela ne dégrade pas la qualité du reste de l'internet en-deçà d'un niveau suffisant.

L'ARCEP présente sa démarche comme préventive, « *les risques portant sur des évolutions potentielles des pratiques davantage que sur des dysfonctionnements actuels du marché* ». Ceci justifie le recours au droit souple, assorti d'une exigence de transparence des opérateurs sur leurs pratiques de gestion de trafic, de la mise en place d'indicateurs portant sur la qualité de service et d'une collecte d'informations sur le marché de l'interconnexion[119]. Les propositions formulées par des parlementaires et par le Conseil national du numérique tendant à inscrire le principe de neutralité du *net* dans la loi[120] n'ont pas eu de suite à ce jour.

C'est en fait du droit de l'Union européenne que sont venus les premiers éléments de reconnaissance de la neutralité du *net* dans le droit positif, et c'est également de lui que pourrait venir sa consécration. Dans le cadre de la transposition du « *troisième paquet télécoms* », l'ordonnance n° 2011-1012 du 24 août 2011 a ajouté à liste des objectifs de la régulation, fixée par l'article L. 32-1 du code des postes et des communications électroniques, ceux de veiller « *à l'absence de discrimination, dans des circonstances analogues, dans les relations entre opérateurs et fournisseurs de services de communications au public en ligne pour l'acheminement du trafic et l'accès à ces services* » et de « *favoriser la capacité des utilisateurs finals à accéder à l'information et à en diffuser ainsi qu'à accéder aux applications et services de leur choix* », objectifs qui ont tous deux trait à la neutralité du *net*. Elle a également étendu les pouvoirs de règlement des différends de l'ARCEP à ceux portant sur les « *conditions réciproques techniques et tarifaires d'acheminement du trafic entre un opérateur et une entreprise fournissant des services de communication au public en ligne* » (article L. 32-8), alors que l'ARCEP ne pouvait auparavant régler que les

119. La décision de l'ARCEP mettant en place cette collecte d'informations a fait l'objet d'un recours des sociétés ATT et Verizon, recours rejeté par le Conseil d'État : cf. CE, 10 juillet 2013, *Société AT&T Global Network Services France SAS et autres*, n° 360397, à mentionner aux tables.

120. Proposition de loi du 20 décembre 2010 relative à la neutralité du *net*, présentée par MM. J.-M. Ayrault, C. Paul et al. ; proposition de loi du 12 septembre 2012 relative à la neutralité de l'internet, présentée par Mme L. de la Raudière ; Conseil national du numérique, avis n° 2013-1 du 1er mars 2013.

différends entre opérateurs. La proposition de règlement établissant des mesures relatives au marché unique européen des communications électroniques et visant à faire de l'Europe un continent connecté, adoptée par la Commission européenne le 11 septembre 2013[121] et qualifiée de « *quatrième paquet télécoms* », comporte une reconnaissance plus large du principe de neutralité du *net.* Son article 23, intitulé « *Liberté de fournir et de se prévaloir des offres d'accès à un internet ouvert, et gestion raisonnable du trafic* », consacre le principe dans des termes très proches de ceux des recommandations de 2010 de l'ARCEP française, mais en leur donnant cette fois-ci une portée contraignante.

Dans sa formulation initiale, le principe de neutralité du *net* visait surtout à définir les obligations des opérateurs de communications électroniques (Tim Wu parlait d'ailleurs de « *network neutrality* », c'est-à-dire littéralement la neutralité du réseau). Les réflexions les plus récentes tendent cependant à élargir la problématique aux questions de neutralité des terminaux et de neutralité des « plateformes »[122], l'expression désignant tous les sites servant de portail d'accès à des contenus fournis par des sites tiers, et recouvrant notamment les moteurs de recherche, les réseaux sociaux, les sites de partage de contenus et les « *magasins d'applications* » utilisés sur les téléphones mobiles. Ces questions, dont les enjeux économiques sont importants (cf. *infra* 1.3.2), amènent à s'interroger sur la nature des moteurs de recherche, deux thèses s'affrontant à cet égard : celle de leur neutralité, le moteur de recherche ne faisant que renvoyer une image de la réalité du *web*, ou au contraire celle de l'affirmation de leur « *liberté éditoriale* »[123] (cf. *infra* 2.2).

1.3. Le numérique a entraîné de profondes modifications du régime juridique de plusieurs libertés fondamentales

Le numérique a ainsi suscité la reconnaissance de nouveaux droits fondamentaux. Il a aussi entraîné de profondes modifications du régime juridique de plusieurs libertés fondamentales préexistantes. L'essor du numérique favorise à l'évidence l'exercice de certains droits, tout en remettant en question certains aspects de leur régime juridique. Ainsi, en bouleversant les moyens de communication, le numérique amène à réexaminer les cadres légaux de la liberté d'expression (1.3.1). Il ouvre de nouveaux espaces à la liberté d'entreprendre, dont il complique la régulation concurrentielle et les réglementations sectorielles (1.3.2). Pour d'autres droits, le numérique se présente davantage comme un risque, suscitant des réactions du législateur pour y parer. Le numérique suscite de nouvelles menaces pour le droit à la sécurité, tout en donnant de nouveaux moyens à la

121. 2013/0309 (COD).

122. Cf. Conseil national du numérique, *Neutralité des plateformes. Réunir les conditions d'un environnement numérique ouvert et soutenable*, mai 2014.

123. Selon l'expression de Cédric Manara, « La *« search neutrality »* : Mythe ou réalité ? », *Concurrences*, n° 1-2011, pp. 52-57.

police administrative, à la police judiciaire et au renseignement, qui appellent de nouvelles garanties pour la liberté personnelle (1.3.3). Enfin, le numérique fragilise le droit de propriété intellectuelle (1.3.4).

1.3.1. La liberté d'expression face au bouleversement des moyens de communication

En bouleversant les moyens de communication, le numérique amène à réexaminer les régimes juridiques de la liberté d'expression, auparavant définis par *medium* (presse écrite et audiovisuel), et suscite des débats sur l'opportunité de reconnaître un nouveau principe, la neutralité du *net*, et sur le contenu qui doit lui être donné. Enfin, si l'essor d'internet ne change pas les limites pouvant être imposées à la liberté d'expression, il amène à s'interroger sur les instruments de la lutte contre les contenus outrepassant ces limites.

La convergence entre la radiodiffusion audiovisuelle et internet entraîne une redéfinition des régimes juridiques de la liberté de communication

Si la liberté d'expression est le principe fondamental commun à tous les moyens de communication, le régime juridique qui en définit les conditions d'exercice n'est pas le même selon le *medium* employé. Jusqu'à l'émergence d'internet, il y avait une parfaite superposition entre la forme d'expression, le moyen technique employé et le régime juridique : la presse, diffusée sous la forme de journaux imprimés et régie par la loi du 29 juillet 1881 sur la liberté de la presse ; la communication téléphonique, assurée par les opérateurs de télécommunications et régie par le code des postes et télécommunications ; la communication audiovisuelle, assurée par radiodiffusion hertzienne, par câble ou par satellite, et régie par la loi du 30 septembre 1986 relative à la liberté de communication. Le régime de la liberté de la presse était marqué par l'absence de contrôle *a priori*, seuls certains abus de la liberté d'expression pouvant être réprimés par le juge pénal ; le régime de la communication téléphonique par le principe de secret de la correspondance ; celui de l'audiovisuel par un régime d'autorisation, en raison de la rareté des fréquences hertziennes, assorti de diverses obligations incombant aux diffuseurs (diffusion de programmes éducatifs et culturels, de programmes en langue française, soutien à la production, etc.). Internet met en question ces distinctions, puisqu'il permet de diffuser par le même *medium* des contenus relevant de la correspondance privée, de la presse et de l'audiovisuel, phénomène souvent qualifié de « *convergence* »[124].

Le droit français a connu de manière récurrente des tentatives de rapprochement des régimes juridiques de la communication sur internet et de l'audiovisuel, qui ne sont jamais vraiment concrétisées.

---

124. Cf. notamment Commission européenne, *Livre vert sur la convergence des secteurs des télécommunications, des médias et des technologies de l'information, et les implications pour la réglementation*, COM (97)623, décembre 1997 ; Commission européenne, *Livre vert « Se préparer à un monde audiovisuel totalement convergent : croissance, création et valeurs »*, COM (2013)231, avril 2013.

- Dès la loi du 30 septembre 1986, la convergence technique est envisagée[125] et la Commission nationale de la communication et des libertés (CNCL) est compétente tant à l'égard du secteur des télécommunications que de celui de l'audiovisuel. Ce choix est cependant remis en cause dès la loi du 17 janvier 1989 : le Conseil supérieur de l'audiovisuel (CSA), nouvelle AAI qui succède à la CNCL, voit ses compétences recentrées sur l'audiovisuel.

- La loi de réglementation des télécommunications de 1996 créait un premier cadre juridique pour les services alors dits « télématiques » consultables sur internet. Elle créait un « *Comité supérieur de la télématique* », placé auprès du CSA, qui devait proposer à l'adoption de ce dernier des recommandations de « règles déontologiques ». Le Conseil constitutionnel a annulé ces dispositions pour incompétence négative du législateur, la loi n'ayant pas encadré le pouvoir de définition de ces règles déontologiques, qui pouvaient donner lieu à des avis de manquement susceptibles d'avoir des incidences pénales (décision n° 96-378 DC du 23 juillet 1996, §28).

- Enfin, le projet de loi pour la confiance dans l'économie numérique, destiné à transposer la directive dite « commerce électronique »[126], définissait initialement la « communication publique en ligne » (c'est-à-dire par internet) comme une sous-catégorie de la communication audiovisuelle. Ce choix a été délibérément écarté par le Parlement[127], qui a défini à l'article 2 de la loi du 30 septembre 1986 modifiée une architecture différente : au sein des « *communications électroniques* », catégorie la plus large, on distingue la « *communication au public par voie électronique* » des communications qui ont le caractère d'une correspondance privée (courriel, téléphone) ; au sein des communications au public par voie électronique, on distingue la « *communication au public en ligne* » (qui correspond au *web*), caractérisée par la possibilité d'un « *échange réciproque d'informations entre l'émetteur et le récepteur* », de la communication audiovisuelle, qui comprend notamment les services de radio et de télévision.

---

125. Selon Gérard Longuet, alors secrétaire d'État à l'industrie : « *Quant à la numérisation générale, elle transforme les images, les données, les sons ou les textes en impulsions de systèmes informatiques, ce qui aboutit à banaliser les données transportées. Ainsi, les secteurs de l'audiovisuel et des télécommunications tendent à se confondre en un seul et même secteur sur le plan technique.* » (discussion générale sur le projet de loi du Gouvernement, 1ère séance du 4 août 1986, JORF n° 72 AN du 5 août 1986, p. 4012).

126. Directive n° 2000/31/CE du Parlement européen et du Conseil du 8 juin 2000 relative à certains aspects juridiques des services de la société de l'information, et notamment du commerce électronique, dans le marché intérieur (directive sur le commerce électronique).

127. Selon les termes du parlementaire Jean Dionis du Séjour : « *Votre rapporteur estime que ce rattachement n'est pas opportun. Un consensus très large s'est dégagé sur ce point parmi les personnes auditionnées en préparant la discussion de ce projet de loi. Aussi bien les acteurs économiques et les industriels du secteur que les milieux associatifs y sont défavorables. (…) Il existe, en effet, entre l'Internet et l'audiovisuel, une différence de nature. Internet repose sur une demande individuelle de l'utilisateur alors que la diffusion audiovisuelle arrive, en tout état de cause, à l'usager qui choisit ou non de les regarder ou de les écouter.* » (rapport fait au nom de la commission des affaires économiques de l'Assemblée nationale, n° 612, 12 février 2003).

Le régime juridique de la liberté d'expression sur internet apparaît relativement stable depuis la publication de la loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique (LCEN). En cohérence avec l'architecture d'internet (cf. *supra* 1.1.1), il encadre de manière distincte la couche des infrastructures et la couche des contenus. Le régime de la couche des infrastructures, défini par le code des postes et des communications électroniques (CPCE) est commun à internet et à ce qu'on appelait, dans l'ancienne terminologie, les télécommunications, les « *opérateurs* », définis comme « *toute personne physique ou morale exploitant un réseau de communications électroniques ouvert au public ou fournissant au public un service de communications électroniques* » (15° de l'article L. 32 du CPCE) et qui peuvent acheminer dans le cadre du même régime juridique des communications téléphoniques et des échanges sur internet.

S'agissant de la couche des contenus, la LCEN a défini deux grandes catégories d'acteurs :

- Les **éditeurs de services sur internet** sont soumis à un régime très voisin de celui de la presse (III à V de l'article 6) : ils ne sont soumis à aucune obligation de déclaration préalable ou d'autorisation ; les seules limites à leur liberté d'expression sont celles définies par le chapitre IV de la loi du 29 juillet 1881, ces infractions étant poursuivies et réprimées selon les conditions définies par le chapitre V de cette même loi ; ils doivent désigner un directeur de publication ; un droit de réponse est prévu par la LCEN, qui transpose à internet le régime défini par l'article 13 de la loi du 29 juillet 1881 pour la presse.

- Les **hébergeurs**, définis comme « *les personnes physiques ou morales qui assurent, même à titre gratuit, pour mise à disposition du public par des services de communication au public en ligne, le stockage de signaux, d'écrits, d'images, de sons ou de messages de toute nature fournis par des destinataires de ces services* » (2. du I de l'article 6), bénéficient d'un régime de responsabilité civile et pénale atténué par rapport à celui des éditeurs, puisqu'ils sont regardés comme n'exerçant pas de contrôle sur les contenus accessibles par leur site : leur responsabilité ne peut être engagée que s'ils avaient connaissance de l'activité illicite ou si, après avoir été informés, ils n'ont pas agi promptement pour retirer le contenu ou le rendre inaccessible[128].

Le régime de la communication sur internet, qu'il s'agisse de celui des éditeurs ou *a fortiori* de celui des hébergeurs, est ainsi marqué par un grand libéralisme, qui le distingue nettement du régime de la communication audiovisuelle, soumise à autorisation préalable et dans lequel des obligations diverses sont imposées aux fournisseurs de contenus. Cette *summa divisio*, dont la stabilité est favorisée par son ancrage dans le droit de l'Union européenne, n'a cependant pas mis fin aux débats sur les conséquences à tirer de la convergence. La convergence technique, pressentie dans les années 1980, est devenue une réalité dans les années 1990 ; la convergence des contenus n'est devenue une réalité qu'au cours des dernières années. En 2003, le rapporteur de la LCEN à l'Assemblée nationale pouvait

128. Une disposition similaire, également issue de la LCEN, est prévue pour les opérateurs de communications électroniques à l'article L. 32-3-3 du CPCE.

encore écrire : « *Internet, c'est d'abord du texte* » ; en juillet 2013, 34 millions de « *vidéonautes* » français ont vu au moins une vidéo sur internet au cours du mois et les vidéos représentent la plus grande part du trafic sur internet. Le développement de la consommation audiovisuelle sur internet, notamment de films et de séries télévisées, conduit à de nouvelles interrogations sur l'écart entre le régime juridique de l'audiovisuel et celui de l'internet : un même contenu peut être soumis à deux régimes très différents selon son mode de diffusion ; cela peut être source de difficultés tant pour les acteurs de l'audiovisuel, qui peuvent y voir une distorsion de concurrence, que pour le soutien à la création et à la production de contenus culturels, qui repose en France largement sur ces acteurs.

C'est pour répondre à ces progrès de la consommation audiovisuelle sur internet que la directive n° 2010/13/UE du Parlement européen et du Conseil du 10 mars 2010, dite « *directive services de médias audiovisuels* », a créé une nouvelle catégorie juridique intermédiaire, celle des « *services de médias audiovisuels à la demande* » (SMAD). Elle a été transposée en France par un décret du 12 novembre 2010. Les SMAD regroupent les services de télévision de rattrapage et de vidéo à la demande. La directive permet de leur imposer certaines des obligations des services audiovisuels sur la diffusion d'œuvres européennes, le soutien à la production et la protection des mineurs. Les débats se poursuivent cependant en raison de la part modérée des SMAD dans la consommation de vidéos en ligne, dominée par les plateformes de partage de contenus tels que *Youtube* ou *Dailymotion* et par les usages illicites, ainsi que de la non-application de ce cadre juridique aux acteurs extraeuropéens (cf. *infra* 1.4 sur la territorialité)[129].

Internet ne modifie pas les limites de la liberté d'expression mais affecte les moyens de lutte contre les contenus illicites

Les textes constitutionnels et conventionnels qui garantissent la liberté d'expression reconnaissent tous la possibilité de lui imposer certaines limites. Selon l'article 11 de la Déclaration des droits de l'homme et du citoyen, « *tout Citoyen peut (…) parler, écrire, imprimer librement, sauf à répondre de l'abus de cette liberté dans les cas déterminés par la Loi* ». L'article 10 de la Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales et l'article 19 du Pacte international des Nations unies relatif aux droits civils et politiques comportent une liste de motifs justifiant que des atteintes puissent être portées à la liberté d'expression (notamment la sécurité nationale, la sûreté publique, la défense de l'ordre ou la protection de la réputation ou des droits d'autrui)[130].

---

129. Cf. notamment CSA, *Rapport au Gouvernement sur l'application du décret n° 2010-1379 du 12 novembre 2010*, novembre 2013 ; contribution française sur le livre vert de la Commission « *Se préparer à un monde audiovisuel pleinement convergent : croissance, création et valeurs* », novembre 2013.

130. L'article 10.2 de la Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales, plus détaillé, stipule que « *l'exercice de ces libertés comportant des devoirs et des responsabilités peut être soumis à certaines formalités, conditions, restrictions ou sanctions prévues par la loi, qui constituent des mesures nécessaires, dans une société démocratique, à la sécurité nationale, à l'intégrité territoriale ou à la sûreté publique, à la*

Par lui-même, internet ne remet en cause ni l'existence de ces limites ni leur tracé. Les textes limitant la liberté d'expression, mentionnés en référence ci-dessus, s'appliquent de plein droit à l'expression sur internet. La LCEN a étendu aux éditeurs de services de communication au public en ligne le chapitre IV de la loi du 29 juillet 1881 relatif aux crimes et délits commis par voie de presse, qui punit notamment la provocation aux crimes et délits, en particulier la provocation à la discrimination ou à la haine envers des personnes en raison de leur origine, de leur religion ou de leur orientation sexuelle, la négation de crimes contre l'humanité, la diffamation, l'injure, ou encore la révélation de l'identité d'agents des services de renseignement.

Pour sa part, la CEDH a développé une jurisprudence assez abondante qui témoigne de sa volonté d'appliquer à internet les principes généraux qu'elle a définis en matière de liberté d'expression, tout en reconnaissant à plusieurs reprises l'existence d'une circonstance aggravante liée à la diffusion sur internet[131]. Selon la jurisprudence constante de la Cour, les ingérences d'autorités publiques dans l'exercice de la liberté d'expression peuvent être admises si elles sont prévues par la loi, inspirées par des buts légitimes au regard de l'article 10.2 de la convention et nécessaires dans une société démocratique pour atteindre ces buts. C'est dans le cadre de cette jurisprudence constante que la Cour a jugé que ne méconnaissaient pas l'article 10 les mesures suivantes : une amende infligée à un élu local ayant publié sur son site internet un appel au boycott des produits israéliens, « *ce message [sur internet ayant] aggravé le caractère discriminatoire de la position du requérant* » (CEDH, 16 juillet 2009, *Willem c. France*, n° 10883/05) ; la condamnation du président du Front national belge pour des propos hostiles aux immigrés tenus sur internet, « *le caractère condamnable d'un message [étant] aggravé par sa diffusion sur internet* » (CEDH, 16 juillet 2009, *Féret c. Belgique*, n° 15615/07) ; l'interdiction par la police d'une campagne d'affichage pour promouvoir le site internet d'une secte en raison des dangers pour les mineurs qui étaient susceptibles d'accéder à ce site et « ***compte tenu du fait que la requérante est en mesure de continuer à diffuser ses idées par le biais de son site internet ainsi que par d'autres moyens à sa disposition, comme la distribution de tracts dans la rue ou dans les boîtes aux lettres*** » (CEDH, Gde Ch., 13 juillet 2012, *Mouvement raëlien suisse c. Suisse*, n° 16354/06). Dans ce dernier arrêt, la CEDH a relevé que « *les moyens modernes de diffusion d'information et le fait que le site était accessible à tous, y compris aux mineurs, auraient démultiplié l'impact d'une campagne d'affichage* ». À l'inverse, elle condamne un État pour violation de l'article 10 lorsque la législation autorisant le blocage d'un site internet n'est pas suffisamment précise, manquant ainsi à

défense de l'ordre et à la prévention du crime, à la protection de la santé ou de la morale, à la protection de la réputation ou des droits d'autrui, pour empêcher la divulgation d'informations confidentielles ou pour garantir l'autorité et l'impartialité du pouvoir judiciaire ». En des termes voisins, l'article 19 du Pacte international des Nations unies relatif aux droits civils et politiques insiste sur les « *devoirs spéciaux* » et les « *responsabilités spéciales* » que comporte l'exercice de la liberté d'expression.

131. Cf. notamment CEDH, « Internet : la jurisprudence de la Cour européenne des droits de l'homme », *Division de la recherche*, 2011 ; F. Tréguer, « Internet dans la jurisprudence de la Cour européenne des droits de l'homme *», Revue des droits et libertés fondamentaux* [en ligne], 20 mai 2013, disponible à l'adresse : http://rdlf.upmf-grenoble.fr/?p=3918.

l'exigence de prévisibilité de la loi et « *n'a pas permis au requérant de jouir du degré suffisant de protection qu'exige la prééminence du droit dans une société démocratique* » (cf. par exemple CEDH, 18 décembre 2012, *Yildirim c. Turquie*, n° 3111/10).

Les spécificités d'internet conduisent aussi à s'interroger sur l'efficacité des mesures prises par les pouvoirs publics à l'encontre des contenus illicites et sur le rôle reconnu aux acteurs privés dans la lutte contre ces contenus. Sur le premier point, il est souvent avancé que les mesures de blocage et de filtrage, passant par une injonction faite aux fournisseurs d'accès à internet de ne plus donner accès à certains sites, seraient inefficaces. Les députés auteurs de la saisine du Conseil constitutionnel contre la LOPPSI 2 soutenaient ainsi, en s'appuyant sur une étude de la Fédération française des télécommunications (FFT), que ces mesures ne permettaient de bloquer que les accès involontaires aux contenus pédopornographiques et entraîneraient le développement de sites spécialisés dans les services de contournement, rendant plus difficile l'action des services de police contre ces sites. Ils n'ont cependant pas été suivis par le Conseil constitutionnel.

Sur le second point la LCEN, qui transpose la directive *commerce électronique* du 8 juin 2000, impose aux intermédiaires techniques que sont les fournisseurs d'accès à internet et les hébergeurs, certaines obligations (mise en place d'un dispositif de signalement des contenus illicites, retrait des contenus signalés), mais exclut toute « *obligation générale de surveillance* ». Lors des débats parlementaires préalables à leur adoption, ces dispositions avaient déjà été contestées comme mettant en place une « *censure privée* » ; le Conseil constitutionnel avait refusé de se prononcer sur cette question, inaugurant à cette occasion sa jurisprudence sur le caractère restreint du contrôle de constitutionnalité en présence d'une loi de transposition d'une directive inconditionnelle et précise[132]. En outre, le rôle effectif des intermédiaires dans l'encadrement des contenus mis en ligne va souvent au-delà. Il peut comporter des engagements volontaires, pris de leur propre initiative ou à l'instigation des pouvoirs publics. Les grandes plateformes telles que *Facebook*, *Twitter*, *Youtube* ou *Dailymotion* définissent ainsi des « *policies* » sur les contenus qu'elles autorisent. Ces règles, qui ont en principe une vocation mondiale, peuvent rejoindre les prescriptions légales (par exemple sur l'interdiction des appels à la violence), les infirmer (en raison des différences d'approche entre les États-Unis et les pays européens sur les limites de la liberté d'expression) ou couvrir des sujets autres que ceux définis par la loi (par exemple sur l'interdiction des images de nudité). En matière de lutte contre la contrefaçon, *Youtube* pratique de fait une surveillance générale des contenus mis en ligne à travers son outil *Content ID* (cf. *infra* 1.3.3). Les pouvoirs publics peuvent inciter les plateformes à prendre de tels engagements, comme dans le programme « *Safer Internet* » conduit par la Commission européenne. Si l'intervention des intermédiaires de l'internet peut apparaître salutaire pour assurer une protection efficace d'intérêts tels que la lutte contre la xénophobie ou la protection des mineurs, elle suscite des débats sur sa légitimité. L'organisation non gouvernementale *European Digital Rights*

132. Décision n° 2004-496 du juin 2004, § 7 à 9.

(EDRi) critique ainsi ce qu'elle qualifie de « *privatisation de l'exécution de la loi* » (« *privatized law enforcement* »)[133], les restrictions à la liberté d'expression ne devant selon elle être prévues que par la loi et ordonnées par les seuls juges.

1.3.2. De nouveaux espaces pour la liberté d'entreprendre, un encadrement juridique devenu plus complexe

Les bouleversements économiques suscités par le numérique (cf. *supra* 1.1.2) ne sont pas restés sans incidence sur le droit des activités économiques, tant sur la liberté d'entreprendre que sur l'encadrement dont elle peut faire l'objet. La liberté d'entreprendre implique aujourd'hui le droit à une existence numérique. Les deux formes d'encadrement dont elle peut faire l'objet, à savoir la régulation générale de la concurrence et les réglementations sectorielles applicables à certaines activités, sont rendues plus complexes par les mutations associées au numérique.

La liberté d'entreprendre implique aujourd'hui le droit à une existence numérique

Selon la jurisprudence constante du Conseil constitutionnel, la liberté d'entreprendre découle de l'article 4 de la Déclaration des droits de l'homme et du citoyen et a ainsi une valeur constitutionnelle. Elle implique le droit pour les entreprises de développer des activités à caractère numérique. La loi et la jurisprudence présentent aujourd'hui plusieurs garanties de ce que l'on pourrait qualifier de « *droit à une existence numérique* » de l'entreprise, qui implique différents attributs : droit à un nom de domaine, droit à fournir des services sur internet, droit d'utiliser certains instruments tels que la publicité, la cryptographie ou les contrats conclus par voie électronique.

Saisi d'une question prioritaire de constitutionnalité contre la disposition législative servant de base à l'attribution des noms de domaine en .fr, le Conseil constitutionnel a jugé « *qu'en l'état actuel des moyens de communication et eu égard au développement généralisé des services de communication au public en ligne ainsi qu'à l'importance prise par ces services dans la vie économique et sociale, notamment pour ceux qui exercent leur activité en ligne, l'encadrement, tant pour les particuliers que pour les entreprises, du choix et de l'usage des noms de domaine sur internet affecte les droits de la propriété intellectuelle, la liberté de communication et la liberté d'entreprendre* » (décision n° 2010-45 QPC du 6 octobre 2010). Alors que dans le système antérieur, les règles d'attribution et de retrait des noms de domaine étaient fixées par le décret et par une charte du nommage adoptée par l'office d'enregistrement du .fr, l'Association française pour le nommage internet en coopération (AFNIC), la loi[134] fixe désormais le principe selon lequel un nom de domaine est attribué au premier demandeur, les exceptions à ce principe, justifiées par des motifs définis par la loi (atteinte à l'ordre public, droits de propriété intellectuelle, etc.), et les conditions dans lesquelles un nom de domaine peut être retiré ; il y a bien un droit au nom de domaine dont le régime est défini par la loi.

133. EDRi, *Human rights and privatized law enforcement*, février 2014.

134. Articles L. 45 à L. 45-8 du code des postes et des communications électroniques.

Le droit de fournir des services à caractère économique sur internet bénéficie du régime général de liberté d'expression sur le réseau, qui ne distingue pas selon que le contenu a ou non une vocation commerciale. En outre, la directive *commerce électronique* du 8 juin 2000, transposée en France par la LCEN, garantit de manière spécifique la liberté de fournir des « *services de la société de l'information* »[135], qui ne peuvent sauf exception être soumis à un régime d'autorisation. Elle favorise la libre circulation de ces services par-delà les frontières nationales, en interdisant aux États de la restreindre pour des motifs correspondant aux matières entrant dans son champ (marché intérieur, établissement des prestataires, communications commerciales, contrats par voie électronique, responsabilité des intermédiaires, etc.). L'absence d'obligation générale de surveillance des hébergeurs facilite l'utilisation de leurs services par les entreprises, puisque les hébergeurs n'ont pas à exercer de contrôle préalable avant la mise en ligne de contenus.

La LCEN facilite également le recours à différents instruments de l'activité économique sur internet. La publicité en ligne est libre, sous réserve de quelques règles destinées à assurer la protection des consommateurs (présentation claire et non équivoque, encadrement de la prospection directe automatisée). Une ordonnance n° 2005-674 du 16 juin 2005 a rendu possible et organisé la conclusion de contrats par voie électronique, celle-ci pouvant être utilisée à tous les stades (échange d'informations sur les conditions du contrat, conclusion du contrat, envoi d'écrits relatifs à l'exécution du contrat)[136]. L'utilisation de moyens de cryptologie, indispensable pour sécuriser les transactions et plus largement l'activité économique, n'est plus soumise à autorisation sauf cas particuliers[137].

La régulation de la concurrence est devenue plus complexe

Tant le droit de l'Union européenne (articles 101 et 102 du Traité sur le fonctionnement de l'Union européenne) que la loi française (articles L. 4201-1 et L. 420-2 du code de commerce) énoncent des règles générales de concurrence applicables à l'ensemble des activités de production, de distribution et de services, qui prohibent les abus de position dominante et les ententes ayant pour objet ou pour effet de fausser le jeu de la concurrence. Ces règles s'appliquent de plein droit aux entreprises de l'économie numérique. Celle-ci pose cependant des questions spécifiques au droit de la concurrence.

---

135. Il s'agit des services « *prestés normalement contre rémunération, à distance par voie électronique et à la demande individuelle d'un destinataire de services* ».

136. Articles 1369-1 à 1369-11 du code civil.

137. Demeurent en revanche soumis à un régime de déclaration préalable auprès du Premier ministre la fourniture, le transfert depuis un État membre de la Communauté européenne ou l'importation d'un moyen de cryptologie n'assurant pas exclusivement des fonctions d'authentification ou de contrôle d'intégrité (c'est-à-dire assurant des fonctions destinées à préserver la confidentialité du message). Le transfert vers un État membre de la Communauté européenne et l'exportation d'un moyen de cryptologie n'assurant pas exclusivement des fonctions d'authentification ou de contrôle d'intégrité sont soumis à autorisation du Premier ministre. Les attributions du Premier ministre en la matière sont exercées par l'Agence nationale de sécurité des systèmes d'information (ANSSI).

On observe d'abord sur de nombreux pans de l'économie numérique une tendance à la concentration du marché autour d'un ou de quelques acteurs prééminents. En 2012, *Google* représentait 94 % des requêtes faites à des moteurs de recherche en France et 65 % dans le monde[138]. Les systèmes d'exploitation des smartphones sont dominés par un duopole formé d'*Android*, développé par *Google* (74 % de parts de marché) et d'*iOS* d'*Apple* (18 %)[139]. Les réseaux sociaux sont marqués par la prééminence de *Facebook* (51 % des internautes l'ont consulté sur un mois en 2013), derrière lequel suivent *Google +* (26 %) et *Twitter* (22 %)[140]. Cette concentration au profit d'acteurs mondiaux s'exerce surtout sur les marchés américains et européens, le marché chinois, premier en nombre d'internautes, étant dominé par des acteurs nationaux (notamment *Baidu*, *Tencent* et *Sina Weibo*).

Plusieurs facteurs peuvent expliquer cette tendance à la concentration. L'économie numérique est marquée par des rendements d'échelle croissants : une fois consentis les investissements, qui peuvent être très lourds, nécessaires à la mise en place d'un service performant, celui-ci peut être fourni à un plus grand nombre d'utilisateurs à un coût marginal presque nul. Certains services connaissent des effets de réseau : il est d'autant plus intéressant de participer à un réseau que le nombre d'utilisateurs est important, et lorsqu'un réseau a acquis une place prééminente, il devient donc difficile de le concurrencer. L'abondance de l'information et de l'offre disponibles sur internet rendent incontournables les « *plateformes* » servant d'intermédiaire et proposant une sélection aux internautes. Selon la formule de Nicholas Carr, « *la réalité du* web *est l'hypermédiation* »[141].

Certes, l'innovation constante que connaît l'économie numérique est susceptible de remettre en cause les positions acquises. *Microsoft* occupait au début des années 2000 la position qu'exerce aujourd'hui *Google* sur les moteurs de recherche. *Nokia* était encore il y a quelques années le premier constructeur mondial de téléphones mobiles. Cependant, la tendance des acteurs dominant aujourd'hui l'économie numérique à étendre constamment leur activité à de nouveaux services et à racheter les acteurs émergents susceptibles de leur faire concurrence pourrait rendre plus difficile à l'avenir la remise en cause de ces positions. La diversification des services offerts par une même entité multiplie les sources de collecte des données personnelles et accroît ainsi la valeur rendue par chaque service.

Face à ces phénomènes susceptibles de constituer des positions dominantes au sens du droit de la concurrence et de donner lieu à des abus, les concepts classiques de la régulation ne sont pas toujours aisés à manipuler. La définition des marchés pertinents, étape incontournable dans l'appréciation portée sur l'existence d'une position dominante, n'est pas aisée : l'innovation dont naissent nombre de services

---

138. ComScore, décembre 2012, http://www.journaldunet.com/ebusiness/le-net/parts-de-marche-des-moteurs-recherche-dans-le-monde.shtml.

139. Gartner, mai 2013, http://www.journaldunet.com/ebusiness/internet-mobile/ventes-smartphone-monde.shtml.

140. *eMarketer*, mai 2013, http://www.emarketer.com/Article/Which-Social-Networks-Growing-Fastest-Worldwide/1009884.

141. N. Carr, « Google in the Middle », *Rough Type*, avril 2009, http://www.roughtype.com/?p=1249.

numériques a justement pour effet de remettre en cause les frontières existantes entre les marchés (cf. *supra* 1.1.2). Les situations évoluent rapidement : dans son avis n° 10-A-29 du 14 décembre 2010 sur le fonctionnement concurrentiel de la publicité en ligne, l'Autorité de la concurrence relevait que la publicité sur les téléphones mobiles en « *était encore à ses débuts* » et que les publicités personnalisées diffusées par *Facebook* n'étaient pas susceptibles de constituer une « alternative crédible » à la publicité liée aux recherches de *Google* ; de tels constats devraient sans doute aujourd'hui être révisés[142]. Le fait que nombre des marchés concernés soient des marchés « *bifaces* », dans lesquels les services sont proposés à deux catégories de clients, de manière gratuite pour une face et payante pour l'autre face, complique aussi l'application des tests économiques réalisés traditionnellement par les régulateurs. On peut penser que dans nombre de cas, ce caractère biface rend les positions dominantes plus difficiles à concurrencer : ainsi, tant que *Google* attire plus de 90 % des requêtes sur les moteurs de recherche en France, il est très difficile à ses concurrents de séduire les annonceurs, même en leur proposant des conditions commerciales très avantageuses.

Plus difficiles à caractériser, les positions dominantes de l'économie numérique soulèvent aussi des questions spécifiques, qui ne se présentent pas dans des secteurs plus traditionnels et qui échappent souvent à la compétence des régulateurs concurrentiels. L'avis du 14 décembre 2010 de l'Autorité de concurrence met en exergue le fait que nombre des problèmes qui lui ont été présentés au cours de ses investigations ne relèvent pas du droit de la concurrence, mais du droit commercial (litiges commerciaux opposant telle ou telle entreprise à *Google* sans mettre en cause le fonctionnement concurrentiel du marché dans son ensemble), du droit des marques (possibilité pour toute entreprise, depuis septembre 2010, d'acheter comme mots-clés sur le service *AdWords* de *Google* des noms de marques appartenant à d'autres entreprises, ce qui conduit les entreprises titulaires à payer plus cher pour acquérir leur propre marque comme mot-clé) ou du droit des données personnelles (conditions d'utilisation par *Google* des données personnelles de ses utilisateurs pour proposer des publicités ciblées plus pertinentes). Ce respect scrupuleux des règles de compétence limite cependant la capacité du régulateur à appréhender la situation de manière globale. Il est par exemple manifeste que les conditions d'utilisation des données personnelles jouent un rôle déterminant dans le jeu concurrentiel ; cette réalité se situe aujourd'hui dans un angle mort de l'activité des AAI, puisque l'Autorité de la concurrence n'est pas compétente pour apprécier le respect de la législation sur les données personnelles et que la CNIL n'a pas à se situer sur un terrain économique. Par ailleurs, les problèmes de concurrence posés par l'activité des grandes plateformes impliquent souvent d'analyser le fonctionnement de leurs algorithmes de classement des contenus, ce que les régulateurs peuvent peiner à faire tant pour des raisons juridiques (ces algorithmes sont protégés par le secret industriel) que du fait de la complexité technique du sujet.

142. Selon le cabinet spécialisé *eMarketer*, *Google* a réalisé en 2013 49,3 % de parts de marché sur la publicité en ligne, contre 17,5 % pour *Facebook*. En 2014, leurs parts respectives seraient de 46,8 % et de 21,7 %. Les progrès de *Facebook* sont tirés par la progression très rapide du marché de la publicité en ligne sur mobile, passé de 11 % des recettes en 2012 à 63 % en 2014.

Ces difficultés ne privent cependant pas l'intervention des régulateurs concurrentiels de toute pertinence. Dans son avis du 14 décembre 2010, l'Autorité de la concurrence a estimé que *Google* était en position dominante sur le marché de la publicité en ligne liée aux recherches, ce qui a dû influer sur l'activité de *Google* qui était ainsi exposé à un plus grand risque de sanction pour abus de position dominante. À la suite de la plainte d'une société dont le compte *AdWords* avait été subitement fermé et qui se trouvait ainsi dans l'incapacité de diffuser des publicités sur *Google*, celle-ci a pris des engagements rendus contraignants par l'Autorité, tendant à une plus grande transparence de sa politique de contenus et de ses procédures de suspension[143]. Au niveau européen, deux procédures concernant d'éventuels abus de position dominante de *Google* sont pendantes, l'une relative à la recherche en ligne et l'autre à son système d'exploitation *Android*. Dans la première procédure, *Google* a soumis des engagements à la Commission, relatifs notamment à la manière dont il traite ses propres services spécialisés (recherche d'actualités, de cartes, d'hôtels, etc.) par rapport à des services concurrents ; la Commission s'est déclarée prête à les accepter et à les rendre contraignants[144]. La durée de cette procédure, qui a débuté en novembre 2010, peut cependant être regrettée compte tenu de la rapidité d'évolution de l'économie numérique. Comme l'indique la Commission, la procédure serait encore plus longue si celle-ci s'engageait dans des sanctions ; mais si, comme cela est probable, les concurrents de *Google*[145] contestent la décision d'acceptation de la Commission, elle pourrait encore durer plusieurs années.

De nombreuses réglementations sectorielles sont fragilisées par le numérique

Outre les règles générales du droit de la concurrence, de nombreuses activités économiques sont soumises à des réglementations sectorielles, justifiées soit par divers motifs d'intérêt public (sécurité, santé publique, bonne utilisation du domaine public, etc.), soit par l'insuffisance de la régulation générale *a posteriori* pour assurer le bon fonctionnement de la concurrence. L'économie numérique bouscule nombre de ces réglementations, dans la mesure où elle confronte les acteurs établis avec de nouveaux acteurs, qui peuvent contester l'applicabilité de la règle sectorielle ou dont le modèle d'affaires repose sur une logique différente. On en trouve des exemples dans le domaine des télécommunications, du livre et de l'assistance aux justiciables.

Depuis 2007, l'ARCEP demande à l'entreprise *Skype* de faire auprès d'elle la déclaration à laquelle elle est selon l'Autorité tenue, en vertu de l'article L. 33-1 du code des postes et des communications électroniques, dès lors qu'elle fournit au public français un service de communications électroniques. L'ARCEP a porté plainte auprès du procureur de la République, l'absence de déclaration préalable étant punie d'un an d'emprisonnement et de 75 000 euros, et une enquête préliminaire a été ouverte en mars 2014. *Skype* fournit un service de « *voix sur IP* »,

143. Décision n° 10-D-30 du 28 octobre 2010, *Navx c/ Google*.

144. Communiqué de la Commission du 5 février 2014.

145. Rassemblés dans une coalition dénommée « *Fair Search* ».

c'est-à-dire que la communication téléphonique est traitée comme un échange de données sur internet au lieu de passer par la réservation d'une ligne comme dans la téléphonie classique. La société *Skype* soutient qu'elle est un simple service en ligne et qu'elle n'est donc pas soumise à cette obligation de déclaration. Au-delà de cette obligation, l'ARCEP cherche à appliquer à *Skype* l'ensemble du régime des opérateurs de télécommunications, ce qui implique notamment l'acheminement des appels d'urgence, la mise en œuvre des moyens nécessaires à la réalisation des interceptions judiciaires et le paiement de la contribution au service public universel. L'enjeu tient également à la concurrence que les services de voix sur IP font aux opérateurs classiques : selon une étude du cabinet Ovum, le développement de la voix sur IP pourrait causer 479 milliards de dollars de pertes cumulées à l'industrie des télécommunications entre 2012 et 2020[146]. La question que soulève le cas de *Skype* pourrait se poser dans les mêmes termes pour d'autres services comme *Viber* ou *Whatsapp*.

Le cas du livre illustre une autre configuration, dans laquelle il n'y a pas de différence de cadre juridique entre les acteurs établis et les nouveaux entrants[147], mais où le législateur cherche à protéger les acteurs établis qui sont menacés par le modèle économique des nouveaux entrants. La vente en ligne de livres imprimés, dont le leader est l'entreprise *Amazon*, a connu des progrès rapides depuis les années 2000, sa part de marché étant passée de 3,2 % en 2003 à 13,1 % en 2011 ; cette progression s'est faite en partie au détriment des librairies, dont la part de marché a chuté sur la même période de 28,5 % à 23,4 %, dans un marché globalement stagnant[148]. Les acteurs de la vente en ligne ne supportent pas les mêmes charges que les libraires en termes de personnel et de loyers ; les libraires sont contraints par leur espace, alors que les marchands en ligne peuvent proposer une offre illimitée. Une proposition de loi tendant à ne pas intégrer la prestation de la livraison à domicile dans le prix unique du livre, dénommée par la presse « *loi anti-Amazon* », a été votée par l'Assemblée nationale et le Sénat ; elle vise à interdire le cumul de la remise de 5 % sur le prix du livre et la gratuité des frais de port, que pratique notamment la société *Amazon*. Son adoption définitive a cependant été retardée par l'exigence de notification de la règle à la Commission européenne, en application de la directive du 22 juin 1998 prévoyant une procédure d'information dans le domaine des normes et réglementations techniques et des règles relatives aux services de la société de l'information.

Le dernier exemple soulève la question des limites d'un monopole d'exercice d'une profession face au développement de nouveaux services numériques. Lancé en 2012, le site *DemanderJustice.com* propose un service automatisé de constitution de dossiers pour les litiges d'un montant inférieur à 10 000 euros devant les juges de proximité et les tribunaux d'instance, qui sont dispensés de ministère

146. Ovum, *The Future of Voice*, http://ovum.com/research/the-future-of-voice/.

147. Une différence de fiscalité existe cependant dans cet exemple, *Amazon* étant établi au Luxembourg et y acquittant un taux de TVA inférieur à celui applicable en France.

148. Chiffres tirés de Sénat, rapport fait au nom de la commission des affaires culturelles et de l'éducation sur la proposition de loi tendant à ne pas intégrer la prestation de la livraison à domicile dans le prix unique du livre, septembre 2013.

d'avocat. Les fondateurs du site, qui ont aussi lancé une filiale SaisirPrud'hommes.com, soutiennent qu'ils contribuent à rééquilibrer le rapport de forces entre les particuliers, qui répugnent à saisir la justice pour de petits litiges, et les entreprises dotées de services juridiques. Dans un jugement du 13 mars 2014, le tribunal correctionnel a relaxé le directeur du site, poursuivi pour exercice illégal de la profession d'avocat, et débouté le conseil de l'ordre des avocats de Paris et le Conseil national des barreaux qui s'étaient constitués partie civile.

Ces sujets ont été abordés jusqu'à présent dans une optique sectorielle, comme si chacun de ces phénomènes était propre au secteur d'activité concerné. Il se dégage pourtant de ces différents exemples, ainsi que d'autres (taxis et VTC[149], vente de médicaments en ligne[150], etc.) des caractéristiques communes : irruption de nouveaux acteurs qui mettent en cause l'équilibre bâti autour d'une réglementation sectorielle, suivie d'une intervention des pouvoirs publics qui tend soit à inclure les nouveaux acteurs dans la réglementation (cas de la téléphonie sur IP), soit à limiter par la réglementation la capacité des nouveaux acteurs à concurrencer les acteurs établis (cas des taxis face aux VTC, des libraires face aux librairies en ligne, des pharmaciens face à la vente de médicaments en ligne, des avocats face aux sites d'assistance juridique en ligne).

1.3.3. Liberté personnelle : de nouvelles garanties face aux nouveaux instruments du droit à la sécurité

La jurisprudence du Conseil constitutionnel distingue depuis 1999[151] la liberté individuelle de la liberté personnelle. La liberté individuelle, dont l'autorité judiciaire est la « *gardienne* » en vertu de l'article 66 de la Constitution, est entendue strictement et consiste dans le droit de ne pas faire l'objet d'une détention arbitraire. La liberté personnelle, proclamée par l'article 2 de la Déclaration des droits de l'homme et du citoyen, est plus large et couvre le droit à la vie privée, l'inviolabilité du domicile, la liberté d'aller et de venir et la liberté du mariage. Si le numérique ne peut par lui-même mettre en cause la liberté individuelle, ses utilisations à des fins de protection de la sécurité peuvent porter atteinte à la liberté personnelle.

Quant au droit à la sécurité, l'article 1er de la loi n° 95-73 du 21 janvier 1995 d'orientation et de programmation relative à la sécurité, le qualifie de « *droit fondamental* »[152]. De plus, « *la prévention d'atteintes à l'ordre public, notamment d'atteintes à la*

149. Cf. *supra* 1.1.2.

150. L'ordonnance n° 2012-1427 du 19 décembre 2012 réserve la vente de médicaments sur internet aux officines de pharmacie. Le Conseil d'État a annulé cette ordonnance en tant qu'elle ne permettait pas de vendre sur internet les médicaments à prescription facultative (CE, 17 juillet 2013, *M. Lailler et autres*, n° 365317, à mentionner aux tables).

151. Décision n° 99-411 DC du 16 juin 1999, *Loi portant diverses mesures relatives à la sécurité routière et aux infractions sur les agents des exploitants de réseau de transport public de voyageurs*, cons. 20.

152. Cette qualification a été réaffirmée à deux reprises par le législateur, à l'occasion de la loi n° 2001-1062 du 14 novembre 2001 de sécurité quotidienne et de la loi n° 2003-239 du 18 mars 2003 pour la sécurité intérieure.

sécurité des personnes et des biens, et la recherche des auteurs d'infractions, sont nécessaires à la sauvegarde de principes et droits de valeur constitutionnelle ». Enfin, « *il appartient au législateur d'assurer la conciliation entre ces objectifs de valeur constitutionnelle et l'exercice des libertés publiques constitutionnellement garanties, au nombre desquelles figurent la liberté individuelle et la liberté d'aller et venir ainsi que l'inviolabilité du domicile* »[153]. La CEDH juge, quant à elle, que les ingérences dans l'exercice du droit à la vie privée doivent être prévues par la loi, qui doit être suffisamment claire et prévisible, et nécessaires dans une société démocratique à la sauvegarde d'un des intérêts énumérés par l'article 8.2 de la convention (sécurité nationale, sûreté publique, bien-être économique du pays, défense de l'ordre et prévention des infractions pénales, protection de la santé ou de la morale ou protection des droits et libertés d'autrui).

Le numérique permet ou favorise de nouveaux types d'atteintes à la sécurité, qui ont nécessité des réponses juridiques. Il donne aussi de nouveaux moyens à la police judiciaire, à la police administrative et au renseignement, qui appellent de nouvelles garanties pour préserver l'équilibre entre sauvegarde de l'ordre public et liberté personnelle.

Les réponses du droit aux nouvelles menaces pour la sécurité liées au numérique

Les atteintes à la sécurité des personnes permises ou favorisées par le numérique sont multiples et diverses. Une typologie est établie par la convention du 23 novembre 2001 du Conseil de l'Europe sur la cybercriminalité, dite « *convention de Budapest* »[154] : elle distingue les « *infractions contre la confidentialité, l'intégrité et la disponibilité des données et systèmes informatiques* », les « *infractions informatiques* », les « *infractions se rapportant au contenu* » (qui ne couvrent dans la convention que les infractions se rapportant à la pornographie enfantine, mais auxquelles on peut rattacher les « *actes de nature raciste et xénophobe commis par le biais de systèmes informatiques* », qui font l'objet d'un protocole additionnel du 28 janvier 2003) et les « *infractions liées aux atteintes à la propriété intellectuelle et aux droits connexes* ». On peut distinguer de manière plus schématique les atteintes à la sécurité qui ont pour cible le numérique, c'est-à-dire qui visent à entraîner le dysfonctionnement d'un système informatique, et celles pour lesquelles le numérique est un moyen de commettre une infraction. Enfin, les menaces contre les intérêts fondamentaux de la nation, tels qu'ils sont définis par l'article 410-1 du code pénal[155] et reconnus par le Conseil constitutionnel[156], méritent un examen particulier.

153. Cf. notamment la décision n° 94-352 DC du 18 janvier 1995, *Loi d'orientation et de programmation relative à la sécurité,* § 2.

154. Cette convention a été ratifiée par 42 États dont 6 États non membres du Conseil de l'Europe, parmi lesquels les États-Unis, le Japon et l'Australie.

155. « *Les intérêts fondamentaux de la nation s'entendent au sens du présent titre de son indépendance, de l'intégrité de son territoire, de sa sécurité, de la forme républicaine de ses institutions, des moyens de sa défense et de sa diplomatie, de la sauvegarde de sa population en France et à l'étranger, de l'équilibre de son milieu naturel et de son environnement et des éléments essentiels de son potentiel scientifique et économique et de son patrimoine culturel.* ».

156. Décision n° 2011-192 QPC du 10 novembre 2011, § 20.

• *Le numérique comme cible des atteintes à la sécurité : atteintes générales*

Les attaques contre les systèmes informatiques peuvent avoir pour but d'accéder à des données confidentielles, de détruire ou d'altérer des données, d'entraver le bon fonctionnement du système ou d'utiliser des ressources informatiques à l'insu de leur détenteur. Elles sont mises en œuvre à travers différents types de logiciels ou de procédés malveillants (cf. encadré). Les motivations et la nature de leurs auteurs sont diverses : elles peuvent émaner d'individus ou d'organisations criminelles, d'entreprises ou d'États ; leur but peut être aussi de manifester une réprobation politique à l'encontre de la cible de l'attaque ou, dans une intention qui se veut alors bienveillante, de déceler des failles de sécurité afin qu'elles soient corrigées (les « *hackers* » qui pratiquent ces intrusions bienveillantes sont qualifiés de « *white hats* », par opposition aux « *black hats* » malveillants). Plusieurs facteurs concourent à une vulnérabilité croissante aux attaques informatiques, notamment la plus grande dépendance des particuliers, des entreprises et des administrations aux technologies numériques, l'interconnexion des terminaux par internet et le développement de l'internet mobile[157].

Lexique des procédés d'attaque informatique

Les **logiciels malveillants** (traduction de l'anglais « *malware* ») forment la catégorie la plus générique : il s'agit de tout programme destiné à nuire aux cibles de l'attaque informatique ; cette catégorie couvre notamment les virus, les vers, les logiciels espions et les chevaux de Troie.

Les **virus** sont des programmes dotés de la capacité de s'insérer dans un programme hôte, de se reproduire et de se propager d'un ordinateur à un autre, à l'image des virus biologiques. Cette capacité de se reproduire n'est pas nécessairement associée à une fonction malveillante, mais l'usage courant du terme virus concerne des logiciels malveillants, qui peuvent entraver le bon fonctionnement du système attaqué, détruire ou altérer des données.

Les **vers** (traduction de l'anglais « *worm* ») sont des programmes autonomes, à la différence des virus, qui ont la capacité de circuler à travers les réseaux sans passer par l'infection d'un programme hôte.

Les **logiciels espions** (dénommés en anglais « *spyware* ») collectent des données pour les envoyer à un tiers, par exemple des numéros de carte bancaire, des mots de passe ou d'autres informations confidentielles. Les « ***keyloggers*** » sont un type particulier de logiciel espion qui récupère les caractères saisis sur un clavier.

Les **chevaux de Troie** exécutent des fonctions à l'insu de l'utilisateur. Ils peuvent permettre la prise de contrôle à distance d'un équipement informatique.

157. Cf. Centre d'analyse stratégique, « Cybersécurité : l'urgence d'agir », *La note d'analyse*, n° 224, mars 2013.

Les « ***botnets*** » sont des groupes d'ordinateurs infectés, qualifiés alors de « *zombies* », dans le but de leur faire accomplir certaines actions, notamment des attaques par déni de service.

Les **attaques par refus de service** (de l'anglais « *distributed denial of service* » ou « *DDoS* ») consistent à bloquer le fonctionnement d'un serveur à partir d'un réseau de machines, le plus souvent en le submergeant de requêtes.

La France a défini de manière précoce des infractions spécifiques pour punir les atteintes aux systèmes informatiques, dénommés « systèmes de traitement automatisé des données » (STAD), dans le cadre de la loi n° 88-19 du 5 janvier 1988 relative à la fraude informatique, dite *loi Godfrain* (aujourd'hui codifiée aux articles 323-1 à 323-7 du code pénal). Elle punit les faits d'accès frauduleux à un STAD, d'entrave à leur fonctionnement ou encore de modification ou de suppression frauduleuse de données. Si les peines prévues ont été récemment relevées par la loi n° 2012-410 du 27 mars 2012 relative à la protection de l'identité, la définition des infractions n'a pas été modifiée ; ceci témoigne, comme pour la notion de données à caractère personnel, de la possible stabilité des textes législatifs face aux évolutions technologiques, lorsqu'ils sont écrits en des termes suffisamment généraux.

Cette approche répressive se double d'une approche préventive lorsque sont en cause des données à caractère personnel. Dès sa première version, la loi du 6 janvier 1978 a mis à la charge du responsable du traitement une obligation générale de sécurité, qui consiste à « *prendre toutes précautions utiles, au regard de la nature des données et des risques présentés par le traitement, pour préserver la sécurité des données et, notamment, empêcher qu'elles soient déformées, endommagées, ou que des tiers non autorisés y aient accès* » (article 34 du texte actuel). Dans le cadre de la transposition du « *troisième paquet télécoms* », l'ordonnance n° 2011-1012 du 24 août 2011 a imposé aux fournisseurs d'accès à internet d'informer la CNIL et les personnes concernées des « *violations de données à caractère personnel* », ce qui est de nature à les inciter à une plus grande vigilance. La proposition de règlement relatif à la protection des données prévoit d'étendre ces obligations à l'ensemble des responsables de traitement. Au-delà du champ des données à caractère personnel, une proposition de directive du 7 février 2013 concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et de l'information dans l'Union[158] énonce une obligation de notification des incidents de sécurité ayant des conséquences sur la sécurité de services essentiels.

158. 2013/0027 (COD).

• *Le numérique comme cible des atteintes à la sécurité : atteintes spécifiques contre les intérêts fondamentaux de la Nation*

L'État n'échappe pas à la dépendance croissante de son fonctionnement aux systèmes d'information : la plupart de ses grandes fonctions, telles que la défense, la sécurité, la santé, l'éducation, la redistribution ou la collecte de l'impôt en sont aujourd'hui tributaires. Il en va de même des « *opérateurs d'importance vitale* » (OIV) définis par le code de la défense[159], tels que les exploitants des grandes infrastructures de télécommunications, de transport ou d'énergie. Les deux derniers livres blancs de la défense[160] ont dès lors souligné la vulnérabilité croissante du pays aux attaques informatiques, pouvant conduire à l'espionnage, à la prise de contrôle ou au sabotage de systèmes d'importance vitale. Cette vulnérabilité résulte notamment du fait que les infrastructures physiques sont aujourd'hui pilotées par des logiciels de supervision et de contrôle (en anglais « s*upervisory control and data acquisition* » ou SCADA) de conception standardisée ; selon l'Agence nationale de sécurité des systèmes d'information (ANSSI), cette tendance a « *apporté aux systèmes industriels les vulnérabilités du monde de l'informatique de gestion* »[161].

En application du premier livre blanc, la direction en charge de la sécurité des systèmes d'information a été transformée par le décret n° 2009-834 en un service à compétence nationale, l'ANSSI, rattachée au secrétariat général de la défense et sécurité nationale (SGDSN), sous la responsabilité du Premier ministre ; ses moyens ont été progressivement renforcés. L'ANSSI est notamment chargée de proposer les règles de protection des systèmes d'information de l'État, de vérifier leur application, de détecter et de réagir aux attaques informatiques et de jouer un rôle de conseil et de soutien auprès des administrations et des OIV. Les propositions du second livre blanc ont été reprises par les articles 21 à 25 de la loi n° 2013-1168 du 18 décembre 2013 relative à la programmation militaire pour les années 2014 à 2019 et portant diverses dispositions concernant la défense et la sécurité nationale. D'une part, le Premier ministre peut désormais fixer des règles de sécurité des systèmes d'information qui s'imposent aux OIV et qu'ils doivent mettre en œuvre à leurs frais. D'autre part, la loi autorise les services de l'État (en pratique, l'ANSSI), en cas d'attaque informatique, à « *procéder aux opérations techniques nécessaires à la caractérisation de l'attaque et à la neutralisation de ses effets en accédant aux systèmes d'information qui sont à l'origine de l'attaque* ».

---

159. Article L. 1332-1 du code de la défense : « *Les opérateurs publics ou privés exploitant des établissements ou utilisant des installations et ouvrages, dont l'indisponibilité risquerait de diminuer d'une façon importante le potentiel de guerre ou économique, la sécurité ou la capacité de survie de la nation, sont tenues de coopérer à leurs frais dans les conditions définies au présent chapitre, à la protection desdits établissements, installations et ouvrages contre toute menace, notamment à caractère terroriste. Ces établissements, installations ou ouvrages sont désignés par l'autorité administrative.* »

160. *Défense et sécurité nationale : le livre blanc*, juin 2008 ; *Livre blanc sur la Défense et la sécurité nationale*, avril 2013.

161. ANSSI, *Maîtriser la SSI pour les systèmes industriels*, janvier 2014.

Une capacité offensive et non plus seulement défensive, certes limitée aux cas de riposte à une attaque et à un objectif de neutralisation de celle-ci[162], est ainsi autorisée par le législateur.

• *Le numérique comme moyen des atteintes à la sécurité*

Le numérique n'est pas à l'origine de formes de délinquance telles que la contrefaçon, l'escroquerie ou la pédophilie, mais il les facilite et en fait apparaître de nouvelles formes. Au-delà de la contrefaçon d'œuvres immatérielles (cf. *infra* 1.3.4), le numérique favorise aussi la contrefaçon de biens matériels, tels que les médicaments, les cosmétiques, les jouets ou les appareils domestiques, dont il facilite la distribution aux consommateurs. De multiples procédés d'escroquerie sont apparus à la faveur du numérique, tels que le « *phishing* », qui consiste à obtenir la communication d'un numéro de carte bancaire en se faisant passer pour une entité administrative ou commerciale, ou les escroqueries commises sur les sites de vente par les particuliers. L'usurpation d'identité est une forme d'escroquerie qui semble s'être particulièrement développée, internet facilitant la collecte d'informations sur les individus et permettant plus aisément de se faire passer pour une tierce personne, par exemple en piratant un compte personnel ouvert sur un site. Internet démultiplie les possibilités de diffusion des images pédopornographiques ; il peut même être un moyen de rentrer en contact avec des victimes.

Face à ces menaces, le législateur a créé ou renforcé plusieurs infractions. La « *LOPPSI 2* » du 14 mars 2011 a créé une infraction spécifique d'usurpation d'identité (article 226-4-1 du code pénal), qu'elle classe parmi les atteintes à la vie privée. Il est précisé que « *l'infraction est punie des mêmes peines lorsqu'elle est commise sur un réseau de communication au public en ligne* », ce qui témoigne des préoccupations du législateur. Pour lutter contre les atteintes aux mineurs, plusieurs délits spécifiques[163] ou circonstances aggravantes de crimes ou de délits[164] ont été définis par le législateur. Des mesures préventives ont également été prévues pour lutter contre la pédopornographie : dans le cadre de la LCEN, les images pédopornographiques font partie des contenus que les hébergeurs sont tenus de retirer lorsqu'ils leur sont signalés ; la « *LOPSSI 2* » a permis à l'autorité administrative d'enjoindre aux fournisseurs d'accès à internet de bloquer l'accès à des sites diffusant de telles images (toutefois, le décret d'application de cette disposition n'a jamais été adopté). Enfin, un office spécialisé a été créé au sein de

162. Il faut noter que le livre blanc de 2013 avait préconisé de manière plus large la constitution d'une « *capacité informatique offensive* », soulignant qu'elle « *enrichit la palette des options possibles à la disposition de l'État* » et « *comporte différents stades, plus ou moins réversibles et plus ou moins discrets, proportionnés à l'ampleur et à la gravité des attaques* ».

163. Propositions sexuelles faites par un majeur à un mineur de moins de 15 ans en utilisant un moyen de communication électronique (article 227-22-1), enregistrement et diffusion d'images pédopornographiques et consultation de sites proposant ces images (article 227-23).

164. Le viol, l'agression sexuelle et la corruption des mineurs font l'objet de circonstances aggravantes lorsque « *la victime a été mise en contact avec l'auteur des faits grâce à l'utilisation, pour la diffusion de messages à destination d'un public non déterminé, d'un réseau de communication électronique* » (respectivement articles 222-24, 222-28 et 227-22).

la direction centrale de la police judiciaire par un décret du 15 mai 2000, l'office central de lutte contre la criminalité liée aux technologies de l'information et de la communication (OCLCTIC).

Les nouveaux moyens donnés par le numérique à la police judiciaire, à la police administrative et au renseignement

Le numérique renforce l'efficacité de moyens d'action de la police qui le précédaient. Il crée aussi, et pourrait créer à l'avenir, des moyens d'action nouveaux. Ces moyens peuvent renforcer l'efficacité tant de la police judiciaire, dont la mission est « *de constater les infractions à la loi pénale, d'en rassembler les preuves et d'en rechercher les auteurs* » (article 14 du code de procédure pénale), que de la police administrative qui a pour tâche la sauvegarde de l'ordre public et la prévention des infractions, et du renseignement, dont la fonction est de collecter des informations utiles à la sécurité nationale.

• *Le numérique renforce l'efficacité de modes opératoires plus anciens*

L'usage des fichiers par la police est très ancien. Le numérique en change cependant la nature, par les facilités de conservation, d'utilisation et d'interconnexion qu'il procure. Ainsi, les fichiers d'antécédents judiciaires (auparavant le système de traitement des infractions constatées (STIC) de la police nationale et le fichier JUDEX de la gendarmerie nationale, désormais fusionnés dans un unique fichier dit « *traitement d'antécédents judiciaires* » (TAJ)) visent à faciliter la recherche des auteurs d'infractions par le recueil d'informations sur leurs précédentes mises en cause. La taille de ces fichiers a connu une forte progression depuis les années 2000 : le nombre de personnes inscrites dans le STIC comme « *mises en cause* » (le STIC contient par ailleurs des données sur les victimes) est passé de 4 millions en 2000 à 6,8 millions en 2013[165]. Le nouveau fichier TAJ compte 12,2 millions de fiches sur des mis en cause, même si ce chiffre recouvre des doubles comptes en raison de la fusion du STIC et de JUDEX. Depuis la loi sur la sécurité intérieure du 18 mars 2003, ces fichiers servent également à des enquêtes administratives, concernant le recrutement à des emplois présentant une sensibilité particulière (notamment les emplois publics ou privés en matière de sécurité et de défense et les emplois impliquant l'accès à des zones protégées en raison de l'activité qui s'y exerce ; plus d'un million d'emplois seraient concernés), l'accès à la nationalité française, l'octroi et le renouvellement de titres de séjour et la nomination et la promotion dans des ordres nationaux. Le fichier des personnes recherchées (FPR), aujourd'hui encadré par le décret n° 2010-569 du 28 mai 2010, est un instrument essentiel de l'activité des services de police et de gendarmerie puisqu'il rassemble les informations relatives à l'ensemble des personnes recherchées, dans le cadre soit de la police judiciaire, soit de législations administratives spécifiques (étrangers, aliénés), soit de la recherche de personnes disparues. Il comptait selon la CNIL un peu plus de 400 000 fiches au 1er novembre 2010. D'autres fichiers servent à la mise en œuvre de mesures préventives, justifiées par la commission antérieure d'infractions ou par d'autres

165. Chiffres tirés de D. Batho et J.-A. Bénisti, *Les fichiers de police*, rapport d'information de la commission des lois de l'Assemblée nationale, mars 2009 et CNIL, *Conclusions du contrôle des fichiers d'antécédents du ministère de l'intérieur*, juin 2013.

incidents : on peut mentionner par exemple le fichier national des interdits de stade (FNIS), qui recense les personnes faisant l'objet d'une interdiction d'accès en raison de leur condamnation pour atteinte à la sécurité des manifestations sportives.

De même, l'usage de données biométriques remonte en France à la fin du XIXe siècle, avec les travaux réalisés par Alphonse Bertillon pour la préfecture de police sur l'anthropométrie, puis sur le recueil des empreintes digitales. Le numérique a cependant facilité de manière considérable la conservation des empreintes et leur comparaison avec des traces collectées dans des affaires. Le nombre de personnes enregistrées dans le fichier national automatisé des empreintes digitales (FNAED) est ainsi passé d'environ 900 000 en 1997 à 3 millions en 2008. Le recueil des empreintes génétiques a connu des progrès encore plus importants, liés à un élargissement du champ des crimes et délits donnant lieu à un enregistrement : alors que la loi n° 98-468 du 17 juin 1998 relative à la prévention et à la répression des infractions sexuelles ainsi qu'à la protection des mineurs, qui a créé le fichier national automatisé des empreintes génétiques (FNAEG), le réservait aux auteurs d'infractions sexuelles, il couvre aussi aujourd'hui les personnes déclarées coupables d'atteintes volontaires à la vie de la personne, de violences volontaires, de trafic des stupéfiants, de vol ou encore de proxénétisme et de traite des êtres humains[166] ; le nombre de personnes enregistrées, de 2 635 en 2002, était de 806 356 en 2008 et de 2 039 874 en 2012.

La vidéosurveillance ou vidéoprotection, qui a commencé à être utilisée en France à la fin des années 1980, reposait au départ sur une technologie analogique et non numérique. Le passage au numérique facilite la conservation et l'exploitation des images : il permet des applications telles que le comptage automatique du nombre de personnes, la détection de mouvements atypiques (par exemple, une personne restant longtemps à un endroit), la reconnaissance d'un visage ou la lecture automatisée des plaques d'immatriculation[167]. La loi distingue la vidéoprotection sur la voie publique, qui est mise en œuvre par les autorités publiques, de celle effectuée dans des lieux et établissements ouverts au public, la seule pouvant être mise en œuvre par des personnes privées[168]. En 2011, le ministère de l'intérieur dénombrait près de 70 000 caméras sur la voie publique autorisées depuis l'adoption du cadre législatif en 1995 ; en outre, 830 000 caméras ont été autorisées dans les lieux ouverts au public tels que les commerces.

• *Le numérique permet des modes opératoires d'investigation inédits*

Dans les exemples présentés ci-dessus, le numérique accroît la facilité d'utilisation et l'efficacité de pratiques qui lui étaient parfois très antérieures. L'essor des communications électroniques a ouvert en revanche des perspectives tout

166. La liste complète des infractions donnant lieu à enregistrement est fixée par l'article 706-55 du code de procédure pénale.

167. Cf. ministère de l'intérieur, de l'outre-mer et des collectivités locales, *Note technique : la vidéoprotection intelligente*, juillet 2008.

168. Le Conseil constitutionnel a censuré des dispositions qui permettaient à des personnes privées de mettre en œuvre des systèmes de vidéoprotection sur la voie publique, aux abords de leurs bâtiments et installations (décision n° 2011-625 DC du 10 mars 2011, § 19).

à fait nouvelles, qui vont bien au-delà de l'interception des communications téléphoniques. L'ensemble de l'activité des individus sur les réseaux numériques est potentiellement enregistrable et susceptible de révéler de très nombreuses informations sur leurs fréquentations, leurs centres d'intérêt, le contenu de leurs échanges ou leur localisation ; ces informations peuvent s'avérer essentielles pour la défense des intérêts fondamentaux de la Nation ou la lutte contre la criminalité. En France, les deux livres blancs sur la défense de 2008 et de 2013 ont fait du développement des capacités de « *renseignement d'origine électromagnétique* » une priorité, en prévoyant une mutualisation des moyens techniques entre les différents services[169]. Les révélations faites depuis juin 2013 par Edward Snowden, ancien consultant de la *National Security Agency* (NSA) américaine, ont mis en évidence l'ampleur de la collecte et de l'exploitation des communications électroniques par les États-Unis et le Royaume-Uni.

La sécurité pourrait aussi bénéficier, comme bien d'autres activités et politiques publiques, des nouveaux modes d'exploitation des données associés au *Big Data* (cf. *supra* 1.1.1). La police utilise déjà des traitements de données, dénommés « *traitements d'analyse sérielle* », pour recouper les informations dont elle dispose sur les différentes affaires et mettre par exemple en évidence un même mode opératoire des personnes recherchées. Il est cependant possible d'aller aujourd'hui bien plus loin : l'exploitation systématique des données disponibles sur les faits de délinquance, de celles produites par les caméras de vidéosurveillance et les lecteurs automatisés de plaques d'immatriculation ou d'informations diverses (localisation des débits de boisson, de chantiers de construction, etc.) permet de prédire la probabilité qu'un fait de délinquance survienne à telle heure et à tel endroit, prédiction qui peut être utilisée pour optimiser le parcours des patrouilles de police. La ville de Memphis, l'une des plus violentes des États-Unis, revendique ainsi grâce à son programme *Blue CRUSH* (*Crime Reduction Using Statistical History*), mis en œuvre par IBM, d'avoir en sept ans fait baisser le nombre de meurtres et de cambriolages de 36 % et les vols de véhicules de 55 %. La police du grand Londres a récemment fait de l'utilisation du *Big Data* l'un des axes de sa stratégie d'usage des technologies[170].

Les nouvelles garanties pour la liberté personnelle rendues nécessaires par ces nouveaux moyens de police et de renseignement

Des garanties ont été instaurées par le législateur afin d'encadrer ces moyens nouveaux des services de police et de renseignement, notamment pour la mise en œuvre des fichiers de sécurité (a), de la vidéosurveillance (b) et de l'interception des communications (c).

---

169. Les services concernés sont la direction générale de la sécurité extérieure (DGSE), la direction centrale du renseignement intérieur (DCRI), devenue la direction générale de la sécurité intérieure (DGSI) en mai 2014, la direction du renseignement militaire (DRM), la direction de la protection et de la sécurité de la défense (DPSD), la direction nationale du renseignement et des enquêtes douanières (DNRED) et le service de traitement du renseignement et d'action contre les services financiers clandestins (TRACFIN).

170. Metropolitan Police, *Total Technology Strategy 2014-2017*.

(a) La version initiale de la loi du 6 janvier 1978 encadrait strictement la constitution de fichiers à des fins de sécurité, puisqu'elle devait faire l'objet d'un avis favorable de la CNIL ou, à défaut, d'un décret pris sur avis conforme du Conseil d'État. La loi du 6 août 2004 a supprimé ces exigences d'avis conforme. Désormais, en vertu de l'article 26 de la loi du 6 janvier 1978 modifiée, les traitements de données intervenant en matière de sécurité[171] doivent être autorisés par arrêté ministériel pris après avis motivé et publié de la CNIL ; ceux de ces traitements qui portent sur des données sensibles ou des données biométriques doivent être autorisés par décret en Conseil d'État. Les fichiers de sécurité doivent respecter les principes énoncés par l'article 6 de la loi (collecte loyale et licite, finalités déterminées, proportionnalité des données traitées et de leur durée de conservation à ces finalités, exactitude) et sont soumis au contrôle de la CNIL dans les conditions définies par l'article 44.

Certains fichiers de sécurité font l'objet d'un régime dérogatoire, préservant leur confidentialité en raison des enjeux pour la sûreté de l'État. Le III de l'article 26 dispose que certains traitements peuvent être dispensés par décret en Conseil d'État de la publication de l'acte les autorisant ainsi que de celle de l'avis de la CNIL[172]. L'article 44 prévoit que ces traitements dispensés de publication peuvent aussi ne pas être soumis au contrôle de la CNIL. Enfin, l'article 41 prévoit un régime spécifique de droit d'accès pour l'ensemble des traitements intéressant la sûreté de l'État, la défense ou la sécurité publique (ensemble plus large que celui des traitements dispensés de publication et qui couvre notamment les fichiers TAJ, FNAED, FNAEG et FPR), souvent qualifié de « *droit d'accès indirect* » mais qui est également un droit de rectification indirect *»*. Le droit d'accès s'exerce par l'intermédiaire de la CNIL, qui désigne un de ses membres ayant la qualité de magistrat pour « *mener les investigations utiles et faire procéder aux modifications nécessaires* » ; les données concernant le requérant ne lui sont communiquées que si la CNIL constate, en accord avec le responsable du traitement, que cette communication ne compromet pas les finalités du traitement. Les garanties dont est assorti ce régime dérogatoire ont été renforcées par la jurisprudence. S'agissant des traitements dont l'acte réglementaire qui les autorise est dispensé de publication, le Conseil d'État, saisi d'un recours contre le décret autorisant le traitement CRISTINA, a jugé que ce décret ne pouvait être communiqué aux requérants mais qu'il devait être transmis au juge afin que celui-ci puisse s'assurer du bien-fondé d'un moyen[173] (CE, 31 juillet 2009, *Association Aides et autres*,

171. Il s'agit plus précisément de deux catégories de traitements : ceux « *qui intéressent la sûreté de l'État, la défense ou la sécurité publique* » et ceux « *qui ont pour objet la prévention, la recherche, la constatation ou la poursuite des infractions pénales ou l'exécution des condamnations pénales ou des mesures de sûreté* ».

172. Ces traitements sont énumérés par le décret n° 2007-914 du 15 mai 2007 modifié et comprennent notamment le traitement CRISTINA mis en œuvre par la DGSI, les traitements mis en œuvre par la DGSE, le traitement STARTRAC mis en œuvre par TRACFIN.

173. En l'espèce le moyen tiré de ce que le texte adopté ne correspondait ni au texte transmis pour avis au Conseil d'État, ni à l'avis du Conseil d'État.

n° 320196, Rec. p. 341). S'agissant du droit d'accès indirect, le Conseil d'État a estimé que lorsqu'un traitement soumis à ce régime contient sur le requérant à la fois des informations susceptibles de porter atteinte aux finalités du traitement et des informations qui ne font pas courir ce risque, la restriction au droit de communication ne doit porter que sur la première catégorie d'informations (CE, Ass., 6 novembre 2002*, M. Moon et Mme Hak Ja Han M,* n° 194295, Rec. p. 380).

(b) Le régime juridique de la vidéosurveillance a été fixé par la loi n° 95-73 du 21 janvier 1995 d'orientation et de programmation relative à la sécurité[174] et il n'a été jugé conforme à la Constitution par le Conseil constitutionnel (décision n° 94-352 DC du 18 janvier 1995) qu'au vu de l'ensemble des garanties qu'il présentait : régime d'autorisation par le préfet, information claire et permanente du public sur l'existence du système de surveillance et sur la personne responsable, interdiction de la visualisation de l'intérieur des immeubles, avis préalable rendu par une commission présidée par un magistrat du siège, exigence que l'autorisation préfectorale précise la qualité des personnes habilitées à visionner les images, droit d'accès de toute personne intéressée, durée de conservation limitée à un mois sauf en cas d'enquête et enfin sanctions pénales de la vidéosurveillance non autorisée. Il a en outre jugé que la vidéosurveillance ne pouvait faire l'objet, en raison de ses risques pour la liberté personnelle, d'un régime de décision implicite d'acceptation. Dans une décision ultérieure, le Conseil constitutionnel a jugé contraires à la Constitution des dispositions qui permettaient à toute personne morale de mettre en œuvre des dispositifs de surveillance au-delà des abords immédiats de ses bâtiments et installations et qui confiaient à des opérateurs privés le soin d'exploiter des systèmes de vidéoprotection pour le compte de personnes publiques, au motif qu'elles rendaient possibles la délégation à une personne privée de compétences de police administrative générale inhérentes à l'exercice de la force publique (décision n° 2011-625 DC du 10 mars 2011, *LOPSSI 2*, §19).

(c) L'histoire du régime juridique de l'interception des communications en France est celle d'un élargissement progressif et encadré. Jusqu'à la loi n° 91-646 du 10 juillet 1991 relative au secret des correspondances émises par la voie des télécommunications, le système français présentait une double fragilité. D'une part, la CEDH avait jugé, dans le prolongement de sa jurisprudence antérieure (cf. encadré ci-dessous), que l'article 81 du code de procédure pénale, qui dispose que « *le juge d'instruction procède, conformément à la loi, à tous les actes d'information qu'il juge utiles à la manifestation de la vérité* » et sur la base duquel la Cour de cassation jugeait légales les écoutes pratiquées sur commission rogatoire, ne répondait pas à l'exigence de prévisibilité de la loi découlant de l'article 8 de la convention sur le droit à la vie privée (CEDH 24 avril 1990, *Kruslin c/ France*, n° 18801/85). D'autre part, les écoutes pratiquées sur réquisition de l'autorité administrative n'avaient aucune base légale et exposaient donc les personnes qui les décidaient ou les mettaient en œuvre à une condamnation pénale pour violation du secret des correspondances.

174. Il est aujourd'hui codifié au titre V du livre II du code de la sécurité intérieure.

La loi du 10 juillet 1991 a précisé le cadre juridique des interceptions judiciaires et créé celui des interceptions administratives.

- Les interceptions judiciaires ne peuvent être mises en œuvre que lorsque la peine encourue est au moins égale à deux ans d'emprisonnement ; la décision d'y procéder est prise pour une durée de quatre mois, renouvelable, et les enregistrements doivent être détruits à l'expiration du délai de prescription de l'action publique[175]. Des dispositions ultérieures sont venues préciser que les correspondances avec un avocat relevant de l'exercice des droits de la défense et les correspondances avec un journaliste permettant d'identifier une source ne pouvaient être retranscrites.

- Les interceptions administratives[176] ne peuvent être autorisées qu'en vue de finalités définies par la loi, notamment la recherche des renseignements intéressant la sécurité nationale, la sauvegarde des éléments essentiels du potentiel scientifique et économique de la France et la prévention du terrorisme et de la criminalité organisée. Elles sont décidées par le Premier ministre, qui définit chaque année le contingent des interceptions pouvant être mises en œuvre, et exécutées sous sa responsabilité par le groupement des interceptions de contrôle (GIC) ; seules les informations correspondant aux finalités définies par la loi peuvent être retranscrites et les retranscriptions doivent être détruites lorsque leur conservation n'est plus indispensable à la réalisation de ces finalités[177]. La loi du 10 juillet 1991 crée en outre une autorité administrative indépendante, la Commission nationale de contrôle des interceptions de sécurité (CNCIS), chargée de veiller au respect de ces dispositions. Les décisions motivées du Premier ministre lui sont communiquées dans les 48 heures ; dans les faits, elles lui sont transmises préalablement à l'interception. Lorsque la CNCIS estime, à la suite de saisine ou d'un contrôle sur l'exécution de l'interception, que le cadre légal n'est pas respecté, elle peut recommander au Premier ministre d'y mettre fin.

Sélection d'arrêts de la CEDH sur les interceptions de communications

La CEDH a fixé les grands principes de sa jurisprudence en la matière dans son arrêt ***Klass et autres c. Allemagne*** (Plén., 6 septembre 1978, n° 5029/71). Elle était saisie d'un recours mettant en cause la législation allemande sur les écoutes décidées par les autorités administratives. Elle juge d'abord que le secret des correspondances protégé par l'article 8 de la convention couvre les communications téléphoniques. Elle estime que « *caractéristique de l'État policier, le pouvoir de surveiller en secret les citoyens n'est tolérable d'après la Convention que dans la mesure strictement nécessaire à la sauvegarde des institutions démocratiques* », mais aussi que « l*es sociétés démocratiques se trouvent menacées de nos jours par des formes très complexes d'espionnage et de terrorisme, de sorte que l'État doit être capable, pour combattre efficacement ces menaces, de surveiller en secret les éléments subversifs opérant sur son territoire* ». La Cour écarte la violation de l'article 10 de la convention au vu de l'ensemble des garanties prévues par la législation

175. Articles 100 à 100-7 du code de procédure pénale.

176. Leur régime est aujourd'hui codifié au titre IV du livre II du code de la sécurité intérieure.

177. Les enregistrements, quant à eux, sont détruits dans un délai de dix jours.

allemande : nécessité d'indices permettant de soupçonner quelqu'un de projeter ou d'avoir accompli des infractions graves, surveillance limitée au suspect et aux personnes avec lesquelles il est en contact, décision par un ministre fédéral habilité par le chancelier, durée limitée à trois mois renouvelable, contrôle a posteriori par une commission composée de parlementaires de la majorité et de l'opposition et par une commission dite « G10 » dont les membres sont nommés par la commission parlementaire et exercent leurs fonctions en toute indépendance.

Elle juge que si le contrôle de telles mesures doit être normalement assuré par le pouvoir judiciaire, les mécanismes prévus par la loi allemande, qui écarte le contrôle judiciaire, présentent des garanties suffisantes, compte tenu de l'indépendance des deux commissions et de la présence de parlementaires de l'opposition.

Dans l'affaire ***Kennedy c. Royaume-Uni*** (18 mai 2010, n° 26839/05), la CEDH était saisie de la requête d'un citoyen britannique qui estimait faire l'objet d'écoutes et qui avait vu sa requête rejetée par la juridiction spécialisée compétente au Royaume-Uni, l'*Investigatory Powers Tribunal* (IPT), ce qui signifiait en vertu de la loi britannique (le *Regulation on Investigatory Powers Act* ou RIPA) soit qu'aucune écoute n'avait été conduite à son sujet, soit qu'elle avait été conduite légalement. Elle a confirmé à cette occasion sa jurisprudence sur ce que recouvre la prévisibilité de la loi dans le cas particulier des interceptions : « *dans le contexte particulier des mesures de surveillance secrète, telles que l'interception de communications, la prévisibilité ne saurait signifier qu'un individu doit se trouver à même d'escompter quand les autorités sont susceptibles d'intercepter ses communications de manière qu'il puisse adapter sa conduite en conséquence* » ; cependant, « *la loi doit user de termes assez clairs pour indiquer à tous de manière suffisante en quelles circonstances et sous quelles conditions elle habilite la puissance publique à prendre pareilles mesures secrètes* ». La loi doit donc fixer notamment la nature des infractions susceptibles de donner lieu à un mandat d'interception, la définition des catégories de personnes susceptibles d'être mises sur écoute ou encore la fixation d'une limite à la durée d'exécution de la mesure.

La Cour estime que la loi britannique présente suffisamment de garanties de prévisibilité. En particulier, elle admet que les mandats du ministre de l'intérieur autorisant les écoutes téléphoniques, d'une durée limitée, puissent être renouvelés indéfiniment, dès lors que chaque renouvellement doit être autorisé par le ministre et que « *les activités criminelles concernées ont une telle ampleur que la planification des opérations pertinentes demande souvent du temps* ». Elle juge que la possibilité pour chaque citoyen de saisir l'IPT lorsqu'il s'estime écouté présente des garanties suffisantes, d'ailleurs plus fortes que celles prévues par d'autres législations qu'elle avait estimées conformes à la Convention, notamment la législation allemande.

Dans l'affaire ***Uzun c. Allemagne*** (2 septembre 2010, n° 35623/05), la CEDH était saisie par un requérant condamné pour avoir participé à des attentats terroristes et qui avait fait l'objet durant l'enquête de la pose d'une balise GPS sous son véhicule. La Cour juge à cette occasion qu'il « *y a lieu de distinguer (…) la surveillance par GPS d'autres méthodes de surveillance par des moyens visuels ou acoustiques qui, en règle générale, sont davantage susceptibles*

de porter atteinte au droit d'une personne au respect de sa vie privée car elles révèlent plus d'informations sur la conduite, les opinions ou les sentiments de la personne qui en fait l'objet » et en déduit que l'exigence de prévisibilité de la loi doit être appréciée de manière moins stricte que pour les interceptions. Elle estime que le code de procédure pénale allemand, qui autorisait la mise en œuvre « *d'autres moyens techniques spéciaux destinés à la surveillance* », répondait à l'exigence de prévisibilité ainsi entendue. Au vu de l'ensemble des circonstances de l'affaire, elle juge qu'il n'y a pas eu de violation de l'article 8 de la convention.

L'essor des communications électroniques a par la suite étendu les possibilités techniques d'interceptions bien au-delà des seules écoutes téléphoniques. Dans un contexte particulièrement marqué par les préoccupations de lutte contre le terrorisme, à la suite des attentats du 11 septembre 2001 aux États-Unis, du 11 mars 2004 à Madrid et de juillet 2005 à Londres, le législateur a souhaité que les autorités administratives et judiciaires puissent avoir accès à ces données. Le Parlement a d'abord étendu, par la loi n° 2004-669 du 9 juillet 2004, le champ des interceptions judiciaires et administratives des télécommunications à l'ensemble des communications électroniques. Il a ensuite créé, dans le cadre de la loi n° 2006-64 du 23 janvier 2006 relative à la lutte contre le terrorisme, une nouvelle procédure de réquisition administrative auprès des fournisseurs d'accès à internet et des hébergeurs, à la seule fin de lutter contre le terrorisme. À la différence des interceptions de sécurité, qui portent sur le contenu de la communication, cette procédure de réquisition ne porte que sur les « *données techniques de connexion* », parfois qualifiées de « *métadonnées* », c'est-à-dire l'identification des personnes utilisatrices des services, les destinataires des communications, la durée de celles-ci et la localisation des équipements terminaux. Les garanties prévues pour la procédure de réquisition des données techniques ne sont pas identiques à celles prévues par la loi du 10 juillet 1991 : la réquisition est autorisée, non par le Premier ministre, mais par une « *personnalité qualifiée* » désignée par la CNCIS et placée auprès du ministre de l'intérieur ; la CNCIS n'est pas appelée à se prononcer sur chaque demande mais elle en est informée, et peut saisir le ministre de l'intérieur si elle estime que le cadre légal n'est pas respecté. Le Conseil constitutionnel a jugé ces dispositions conformes à la Constitution (décision n° 2005-532 DC du 19 janvier 2006).

Une nouvelle étape est intervenue avec la loi n° 2013-1168 du 18 décembre 2013 de programmation militaire (LPM) et la loi n° 2014-372 du 28 mars 2014 relative à la géolocalisation. L'enjeu de ces deux textes a d'abord été de clarifier le régime juridique de la géolocalisation et notamment de la géolocalisation en temps réel, dont les possibilités se sont beaucoup étendues avec le développement de l'internet mobile. La Cour de cassation avait en effet jugé, dans deux arrêts du 22 octobre 2013, que « *la technique dite de « géolocalisation » constitue une ingérence dans la vie privée dont la gravité nécessite qu'elle soit exécutée sous le contrôle d'un juge* », c'est-à-dire d'un juge du siège[178]. Quant aux autorités administratives, les

178. Cet arrêt s'inscrit dans la jurisprudence de la CEDH (29 mars 2010, *Medvedyev c. France*, et 23 novembre 2011, *Moulin c. France*) et de la Cour de cassation (Crim., 15 décembre 2010, n° 10-83764) selon laquelle les membres du parquet ne remplissent pas en France l'exigence

dispositions issues de la loi du 23 janvier 2006 ne leur permettaient pas clairement de procéder à la géolocalisation en temps réel. La loi relative à la géolocalisation définit les infractions pour lesquelles la géolocalisation peut être mise en œuvre et les conditions de contrôle par le juge d'instruction ou le juge des libertés et de la détention. L'article 20 de la LPM aligne le régime de la géolocalisation en temps réel décidée par l'autorité administrative sur celui des interceptions de sécurité. À cette occasion, le Parlement a aussi procédé à un rapprochement du cadre juridique des interceptions de sécurité et de celui des réquisitions de données techniques de connexion. Auparavant réservées à la lutte contre le terrorisme, ces dernières pourront désormais être faites pour l'ensemble des finalités prévues pour les interceptions de sécurité et la personnalité qualifiée sera placée auprès du Premier ministre.

1.3.4. Le droit de la propriété intellectuelle confronté aux usages des réseaux

Le droit de la propriété intellectuelle est reconnu par plusieurs textes internationaux. L'article 15 du pacte des Nations Unies relatif aux droits économiques sociaux et culturels du 16 décembre 1966 stipule que les États « *reconnaissent à chacun le droit (…) de bénéficier de la protection des intérêts moraux et matériels découlant de toute production scientifique, littéraire ou artistique dont il est l'auteur* ». La propriété littéraire et artistique, en particulier[179], fait l'objet d'une convention internationale très ancienne, la convention de Berne du 9 septembre 1886. La valeur supralégislative du droit de la propriété intellectuelle lui est aussi reconnue en tant que composante du droit de propriété. Le Conseil constitutionnel a jugé « *que les finalités et les conditions d'exercice du droit de propriété ont subi depuis 1789 une évolution caractérisée par une extension de son champ d'application à des domaines nouveaux* » et « *que, parmi ces derniers, figurent les droits de propriété intellectuelle et notamment le droit d'auteur et les droits voisins* » (décision n° 2006-540 DC du 27 juillet 2006, *Loi relative au droit d'auteur et aux droits voisins dans la société de l'information*, § 15). De même, la CEDH a jugé que l'article 1er du protocole n° 1 additionnel à la convention, relatif au droit de propriété, « *s'applique à la propriété intellectuelle en tant que telle* » (CEDH, Gde Ch., 11 janvier 2007, *Anheuser-Busch c. Portugal*, n° 73049/01, §72). L'article 17 de la Charte des droits fondamentaux de l'Union européenne, relatif au droit de propriété, précise en son point 2 que « *la propriété intellectuelle est protégée* ».

Le champ du droit de la propriété intellectuelle a été étendu aux œuvres numériques (logiciels et bases de données) et aux usages numériques des œuvres culturelles (numérisation et diffusion sur internet). Internet en fait cependant largement

---

d'indépendance à l'égard de l'exécutif permettant de les considérer comme des « *magistrats* » au sens de l'article 5.3 de la convention.

179. On distingue classiquement en droit de la propriété intellectuelle le droit de la propriété littéraire et artistique, qui couvre les droits d'auteur et les droits voisins, du droit de la propriété industrielle, qui couvre les marques, dessins et modèles ainsi que les brevets. Cette distinction est reprise dans le plan du code de la propriété intellectuelle.

abstraction en facilitant de manière considérable la reproduction et la diffusion des œuvres en méconnaissance du droit d'auteur et des droits voisins ; les pouvoirs publics ont réagi en combinant prévention, répression et promotion des usages licites. Si des modèles alternatifs, reposant sur la libre réutilisation des œuvres et des logiciels, se développent, leur place dans le droit positif reste à définir.

Le droit de la propriété intellectuelle a étendu son champ aux œuvres et aux usages numériques

Le droit de la propriété intellectuelle a été étendu à des objets issus des technologies numériques, les logiciels et les bases de données ; il joue ainsi dans l'économie numérique un rôle structurant. Les prérogatives classiques du droit d'auteur, que sont le droit de reproduction et le droit de représentation, ont montré leur plasticité en s'appliquant à la numérisation et à la diffusion sur internet.

Bien que les logiciels soient étrangers aux préoccupations esthétiques qui animent traditionnellement le droit d'auteur, « *droit des belles formes* » selon l'expression du professeur Christophe Caron[180], la reconnaissance de leur protection a été précoce. La loi n° 85-660 du 3 juillet 1985 a inclu le logiciel dans la liste des œuvres protégées par le droit d'auteur[181]. Un arrêt *Atari* de l'Assemblée plénière de la Cour de cassation (Ass. Plen., 7 mars 1986, n° 84-93509) est allé dans le même sens, sans avoir à se fonder sur cette disposition spécifique postérieure à l'affaire jugée : alors que la cour d'appel de Paris avait refusé la protection du droit d'auteur à un jeu vidéo, au motif « *que quelle que soit la complexité technique, surtout aux yeux d'un profane, d'un logiciel il s'agit en définitive d'un assemblage technologique qu'il n'y a pas lieu de sacraliser au point de le hisser au rang des œuvres de l'esprit prévues par la loi de 1957 précitée* », la Cour de cassation a jugé que « *la protection légale s'étend à toute œuvre procédant d'une création intellectuelle originale indépendamment de toute considération d'ordre esthétique* ». La protection du logiciel par le droit d'auteur bénéficie principalement à l'entreprise au sein de laquelle il a été élaboré : la loi dispose que les droits patrimoniaux sur les logiciels créés par des employés dans l'exercice de leurs fonctions ou d'après les instructions de leur employeur sont dévolus à l'employeur qui est seul habilité à les exercer[182].

Les bases de données, qui peuvent être protégées par le droit d'auteur lorsqu'elles constituent des créations intellectuelles originales, ont fait l'objet en vertu de la directive n° 96/9/CE du Parlement européen et du Conseil du 11 mars 1996 d'une protection complémentaire, destinée à protéger leurs producteurs, qui ont consenti des investissements pour la constitution de la base. Les auteurs de la directive sont partis du constat que « *la fabrication de bases de données exige la mise en œuvre de ressources humaines, techniques et financières considérables, alors qu'il est possible de les copier ou d'y accéder à un coût très inférieur à celui qu'entraîne une conception autonome* » et « *qu'un tel investissement dans des systèmes modernes de stockage et de traitement de l'information ne se fera pas dans la Communauté*

180. C. Caron, *Droit d'auteur et droits voisins*, LexisNexis, 3e édition, 2013, Paris, p. 1..
181. Cf. aujourd'hui le 13° de l'article L. 112-2 du code de la propriété intellectuelle.
182. Article L. 113-9 du code de la propriété intellectuelle.

en l'absence d'un régime juridique stable et homogène protégeant les droits des fabricants de bases de données ». La directive a été transposée en France par une loi du 1er juillet 1998[183]. Si la loi reconnaît au producteur un monopole sur l'extraction et la réutilisation des données contenues dans la base, la Cour de cassation a jugé, en combinant droit de la propriété intellectuelle et droit de la concurrence, que « *si le titulaire d'un droit de propriété intellectuelle sur une base de données peut légitimement prétendre à une rémunération, il ne peut, lorsque cette base de données constitue une ressource essentielle pour des opérateurs exerçant une activité concurrentielle, subordonner l'accès à cette base de données au paiement d'un prix excessif* » (Com., 4 décembre 2001, n° 99-16-642)[184].

Le droit d'auteur confère de manière classique à son titulaire deux grandes catégories de droits patrimoniaux : le droit de représentation, la représentation consistant dans « *la communication de l'œuvre au public par un procédé quelconque* », et le droit de reproduction, celle-ci étant définie comme « *la fixation matérielle de l'œuvre par tous procédés qui permettent de la communiquer au public d'une manière indirecte* »[185]. Ces droits avaient déjà montré tout au long du XXe siècle leur capacité d'accueil des évolutions techniques, le juge appliquant au cinématographe et aux phonogrammes[186] le droit de reproduction et la loi du 3 juillet 1985 étendant à la télédiffusion le droit de représentation. Dès 1996, la jurisprudence a appliqué de même à la numérisation et à la diffusion sur internet les droits de reproduction et de représentation : par deux ordonnances du 14 août 1996, le juge des référés du tribunal de grande instance de Paris a jugé que la numérisation d'œuvres de Jacques Brel et de Michel Sardou et leur mise à disposition par des étudiants sur les pages *web* du site de leur école portait atteinte aux droits de reproduction et de diffusion et était constitutive d'un acte de contrefaçon[187].

Face au défi des usages illicites, les pouvoirs publics se sont efforcés de combiner l'empêchement et la répression de ces usages avec la promotion des usages licites

Il n'y avait donc pas de difficulté juridique à ce que le droit d'auteur, qui est par nature un droit de l'immatériel, s'étende aux usages du numérique. C'est un défi matériel que le numérique a présenté au droit d'auteur, en facilitant de manière considérable la reproduction et la diffusion des œuvres culturelles et en créant des habitudes de consommation gratuite (cf. *supra* 1.1.2). Face à ce défi, les pouvoirs publics, en France mais aussi dans l'ensemble de l'Europe et aux États-Unis, ont réaffirmé le droit d'auteur et les droits voisins et l'exigence de leur protection. Ils ont adopté des mesures pour empêcher la contrefaçon et la réprimer. Plusieurs

183. Cf. article L. 112-3 pour la protection des bases de données par le droit d'auteur et titre IV du livre III de la première partie pour le droit spécifique des producteurs de bases de données.
184. Le litige opposait *France Télécom* et des sociétés de marketing direct, au sujet des conditions de cession de ses listes d'abonnés.
185. Cf. respectivement les articles L. 122-2 et L. 122-3 du code de la propriété intellectuelle.
186. C'est-à-dire les produits résultant de la fixation sur tout support d'une séquence de sons.
187. *Éditions musicales Pouchenel et autres c/ École centrale de Paris, École nationale supérieure des télécommunications, Jean-Philippe R. et autres*.

écisions juridictionnelles ont cependant affirmé la nécessité de concilier la protection de la propriété intellectuelle avec les exigences découlant d'autres droits fondamentaux, notamment la liberté d'expression et la liberté d'entreprendre. Un autre volet de l'action des pouvoirs publics a été d'encourager et de rendre plus attractifs les usages numériques licites.

• *L'exigence de protection du droit d'auteur et les efforts d'empêchement, de détection et de répression des usages illicites*

L'application du droit d'auteur aux usages des réseaux numériques a été affirmée dès les débuts de l'utilisation d'internet par le grand public. Deux traités de l'Organisation mondiale de la propriété intellectuelle (OMPI) du 20 décembre 1996, sur le droit d'auteur d'une part et sur les interprétations et exécutions et les phonogrammes d'autre part, affirment le droit exclusif des ayants droit « *d'autoriser toute communication au public de leurs œuvres par fil ou sans fil, y compris la mise à la disposition du public de leurs œuvres de manière que chacun puisse y avoir accès de l'endroit et au moment qu'il choisit de manière individualisée* ». Ils imposent aux États parties d'assurer la protection juridique des « *mesures techniques efficaces* » : cette expression désigne les techniques destinées à entraver les utilisations non autorisées des œuvres (codes d'accès, cryptage, limitation du nombre de copies, etc.). Ces traités sont mis en œuvre par les États-Unis, dans le cadre du *Digital Millenium Copyright Act* (DMCA) du 28 octobre 1998 et dans l'Union européenne, par la directive n° 2001/29/CE du Parlement européen et du Conseil du 22 mai 2001 sur l'harmonisation de certains aspects du droit d'auteur et des droits voisins dans la société de l'information (dite *directive DADVSI*).

En France, cinq lois successives ont mis en place les éléments d'une architecture destinée à empêcher les actes commis en méconnaissance du droit d'auteur (a), à les détecter (b) et à les réprimer de manière graduée (c) :

(a) La loi n° 2006-961 du 1er août 2006, dite *loi DADVSI*, a transposé les dispositions de la directive du même nom relatives aux mesures techniques de protection[188]. Les titulaires de droits ont le droit de recourir aux mesures techniques et notamment de limiter le nombre de copies, tout en veillant à respecter les exceptions au droit d'auteur et aux droits voisins[189], notamment l'exception pour copie privée, et à ne pas entraver « l'interopérabilité » entre les différents supports et les équipements permettant de les lire. La loi du 1er août 2006 a instauré des sanctions pénales punissant le fait de porter atteinte à une mesure technique ou de proposer des

188. Parfois dénommées selon l'acronyme de « *DRM* », qui correspond à l'expression anglaise de « *Digital Rights Management* ».

189. Les exceptions au droit d'auteur et aux droits voisins, définies respectivement aux articles L. 122-5 et L. 211-3 du code de propriété intellectuelle, désignent les utilisations que les ayants droit ne peuvent interdire. Elles comportent notamment les exceptions pour usage privé dans un cercle de famille, pour copie privée, de courte citation, de parodie et de pastiche, ainsi que l'exception pour des utilisations au bénéfice de personnes handicapées. Pour être licite, une exception doit satisfaire au « *test en trois étapes* » : elle doit figurer dans la liste et en outre ne pas porter atteinte à l'exploitation normale de l'œuvre ou des objets concernés et ne pas causer un préjudice injustifié aux intérêts légitimes des titulaires de ces droits.

moyens destinés à porter une telle atteinte. Elle a créé une autorité administrative indépendante, l'Autorité de régulation des mesures techniques, chargée de veiller à ce que ces mesures ne portent pas atteinte à l'interopérabilité et de trancher les différends liés à leur mise en œuvre ; ces attributions ont été transférées par la loi n° 2009-669 du 12 juin 2009 à la Haute Autorité pour la diffusion des œuvres et la protection des droits sur internet (HADOPI).

La loi du 1er août 2006 s'est également attachée à empêcher les pratiques illicites en créant un délit de diffusion de logiciels « *manifestement destinés à la mise à disposition du public non autorisée d'œuvres ou d'objets protégés* »[190]. Une condamnation est intervenue à ce jour, à l'encontre de *Radioblog*, un site de musique en « *streaming* » qui a compté jusqu'à 800 000 visiteurs par jour[191].

(b) La LCEN du 21 juin 2004 prévoit un mécanisme général de notification des contenus illicites aux hébergeurs, qui s'applique notamment aux contenus méconnaissant le droit d'auteur. Les ayants droit peuvent ainsi exercer leur vigilance sur les sites de partage de contenus et en obtenir le retrait ; dès lors qu'une notification est faite dans les conditions définies au point 5 du I de l'article 6 de la LCEN, les hébergeurs peuvent engager leur responsabilité civile et pénale s'ils ne procèdent pas au retrait.

La loi du 6 août 2004 relative à la protection des données à caractère personnel a autorisé les sociétés de perception et de répartition des droits d'auteur et des droits des artistes-interprètes et des producteurs de phonogrammes et de vidéogrammes[192], ainsi que les organismes de défense professionnelle[193], à constituer des traitements de données à caractère personnel relatifs aux infractions ; elles peuvent ainsi enregistrer les adresses IP des personnes qui procèdent sur internet à des actes d'utilisation d'œuvres non autorisés par les ayants droit. Il s'agit des seules personnes poursuivant un intérêt privé que la loi autorise à mettre en œuvre un tel traitement. Le Conseil constitutionnel l'a admis en prenant en compte « *l'objectif d'intérêt général qui s'attache à la sauvegarde de la propriété intellectuelle et de la création culturelle* » (décision n° 2004-499 DC du 29 juillet 2004, § 13). Dans le cadre du système de lutte contre le téléchargement de pair à pair de fichiers couverts par le droit d'auteur mis en place par la loi du 12 juin 2009, la HADOPI, saisie par les ayants droit qui ont collecté les adresses IP, demande aux fournisseurs d'accès à internet d'identifier les titulaires d'abonnement correspondants, ce qui permet de mettre en œuvre à leur encontre le dispositif de « *réponse graduée* ».

---

190. Article L. 335-2-1 du code de propriété intellectuelle.

191. CA Paris, 22 mars 2011, confirmé par Crim. 25 septembre 2012.

192. Il s'agit par exemple en France de la Société des auteurs, compositeurs et éditeurs de musique (SACEM), de la Société des auteurs et compositeurs dramatiques (SACD), de la Société civile pour l'administration des droits des artistes et musiciens-interprètes (ADAMI) et de la Société civile pour l'exploitation des droits des producteurs phonographiques (SCPP).

193. L'article L. 331-1 du code de la propriété intellectuelle dispose que « *les organismes de défense professionnelle régulièrement constitués ont qualité pour ester en justice pour la défense des droits dont ils ont statutairement la charge* ».

(c) Le délit de contrefaçon, qui punit de trois ans d'emprisonnement et de 300 000 euros d'amende la diffusion ou la reproduction d'œuvres en méconnaissance des droits d'auteurs et des droits voisins, est applicable aux usages numériques tels que le téléchargement direct, le téléchargement de pair à pair ou le versement de fichiers sur des sites les mettant à la disposition du public. Dès le début des années 2000, des condamnations pénales ont été prononcées sur ce fondement à l'encontre d'internautes participant à ces échanges, notamment à l'initiative de sociétés de gestion collective.

Toutefois, cette sanction est vite apparue inappropriée, en raison de sa sévérité et de la lourdeur de sa mise en œuvre, à la lutte contre des pratiques de masse[194]. La loi DADVSI votée par le Parlement exemptait du délit de contrefaçon et punissait d'une simple contravention les échanges opérés dans le cadre d'un téléchargement de pair à pair. Le Conseil constitutionnel a censuré cette disposition comme contraire au principe d'égalité (décision n° 2006-540 DC du 27 juillet 2006, § 65). Les lois n° 2009-669 du 12 juin 2009 et n° 2009-1311 du 28 octobre 2009 ont mis en place une nouvelle approche, dite de « *réponse graduée* », placée sous la responsabilité d'une instance spécifique de la HADOPI, la commission de protection des droits. Les personnes dont il a été détecté, selon les modalités décrites ci-dessus, que leur abonnement à internet avait servi au téléchargement de pair à pair d'œuvres protégées, se voient adresser deux avertissements, le premier par voie électronique, le second par lettre avec avis de réception ; à la troisième réitération, la commission de protection des droits peut saisir le parquet en vue de leur condamnation pour « *négligence caractérisée* » ; cette infraction constitue une contravention de cinquième classe, que le juge peut assortir d'une suspension de l'accès à internet d'une durée maximale d'un mois[195].

• *Les limites rencontrées par la politique d'empêchement, de détection et de répression graduée*

Le bilan de ces efforts est contrasté. S'agissant des mesures techniques de protection, elles n'ont pas répondu aux espoirs placés en elle. En juin 2005, le rapport fait au nom de la commission des affaires culturelles de l'Assemblée nationale sur la loi DADVSI, affirmait ainsi : « *Pour une grande partie des ayants droit, et plus particulièrement pour les éditeurs de phonogrammes, titulaires de droits voisins, la voie la plus prometteuse, et en l'occurrence déjà mise en œuvre, consiste en la généralisation de l'implantation de mesures techniques de protection sur les supports physiques ou les fichiers dématérialisés* ». En réalité, les mesures techniques ont pu être contournées par les internautes, sans que les dispositions sanctionnant ces contournements soient effectivement appliquées.

L'implication des fournisseurs d'accès à internet et des hébergeurs s'est heurtée à la règle, prévue par la directive « *commerce électronique* » et la loi française, selon laquelle il ne peut leur être imposé « *d'obligation générale de surveillance* ». Dans

194. Cf. par exemple en ce sens D. Barella, « Dépénaliser la musique téléchargée », *Libération*, 14 mars 2005.

195. Cette sanction, qui n'a été prononcée qu'une fois depuis la création de la HADOPI, a été supprimée par le décret n° 2013-596 du 8 juillet 2013.

deux arrêts *Scarlet c/ SABAM* et *SABAM c/ Netlog*, la Cour de justice de l'Union européenne a jugé que les dispositions combinées des directives applicables[196] s'opposaient à ce qu'une juridiction nationale enjoigne à un fournisseur d'accès (dans l'affaire *Scarlet*) ou à un hébergeur (dans l'affaire *Netlog*) de mettre en place un dispositif de filtrage généralisé capable d'identifier des fichiers qui lui soient signalés par les ayants droit (CJUE 24 novembre 2011, C-70/10 et 16 février 2012, C-360/10). Elle a jugé à cette occasion que « *la protection du droit fondamental de droit de propriété, dont font partie les droits liés à la propriété intellectuelle, doit être mise en balance avec celle d'autres droits fondamentaux* », notamment la liberté d'expression, la liberté d'entreprendre et le droit à la protection des données personnelles. Dans le même esprit, la Cour de cassation a jugé dans trois arrêts du 12 juillet 2012 (Civ 1re, n° 11-15.165 et autres) qu'il ne pouvait être imposé à un hébergeur de veiller à ce qu'un contenu qui lui a été signalé comme illicite et qu'il a retiré ne réapparaisse pas à une autre adresse, car cela reviendrait à lui imposer une obligation générale de surveillance, dès lors que les mesures prescrites n'étaient pas limitées dans le temps. Les ayants droit sont donc contraints de procéder à chaque fois à une nouvelle notification. Cependant, certains hébergeurs[197] proposent spontanément aux ayants droit de procéder à un tel filtrage ; en effet, la directive « *commerce électronique* » interdit qu'il soit imposé aux intermédiaires techniques de procéder à une surveillance générale, mais elle ne leur interdit pas d'y procéder de manière volontaire.

Quant à la répression, elle a conduit à la condamnation et à la fermeture de quelques sites très fréquentés, notamment aux États-Unis (*Napster* en 2001, *Megaupload* en 2012) ou en France (fermeture du site *Planète-Lolo* en 2012 à la suite de la mise en examen de ses administrateurs, jugement *Allostreaming* du TGI de Paris du 28 novembre 2013 enjoignant[198] à une série de fournisseurs d'accès à internet et de moteurs de recherche de bloquer et de déréférencer ce site et des sites associés). Les procédures sont cependant longues (le TGI de Paris a mis près de deux ans à statuer dans l'affaire *Allostreaming*), alors que les sites peuvent

196. Il s'agit des directives « *commerce électronique* » et « *DADVSI* », de la directive n° 2004/48/CE du Parlement européen et du Conseil du 29 avril 2004 relative au respect des droits de propriété intellectuelle, de la directive n° 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données et enfin de la directive n° 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (dite « *directive vie privée et communications électroniques* »).

197. Par ex., *Youtube*, avec son service « *ContentID* », ou *Dailymotion* avec « *AudibleMagic* » ou la technologie « *Signature* » développée par l'Institut national de l'audiovisuel (INA).

198. Sur le fondement de l'article L. 336-2 du code de la propriété intellectuelle, en vertu duquel « *le tribunal de grande instance, statuant le cas échéant en la forme des référés, peut ordonner à la demande des titulaires de droits sur les œuvres et objets protégés (…) toutes mesures propres à prévenir ou à faire cesser une telle atteinte à un droit d'auteur ou un droit voisin, à l'encontre de toute personne susceptible de contribuer à y remédier* ».

être reconstitués rapidement. La « *réponse graduée* », qui s'adresse aux simples utilisateurs et non aux responsables des sites mettant en ligne les contenus illicites, a été massivement mise en œuvre : depuis 2010, la commission de protection des droits a émis près de 2,8 millions de « *premières recommandations* », 284 000 « *deuxièmes recommandations* » et délibéré un peu mois de 1 000 fois sur les suites à donner à une troisième réitération[199]. Ces chiffres suggèrent un effet dissuasif des recommandations. Toutefois, la réponse graduée ne couvre que le téléchargement de pair à pair et non le téléchargement direct ou le « *streaming* ». Selon les études réalisées par la HADOPI sur les usages en ligne, le « *streaming* » illicite est le mode d'accès aux biens culturels le plus utilisé par les internautes et il est perçu comme le moins risqué juridiquement. Les pouvoirs publics, inquiets d'un éventuel effet de report du pair à pair vers le « *streaming* » illicite, ont en conséquence sollicité plusieurs rapports pour développer la lutte contre ce dernier[200].

• *La promotion des usages licites*

La promotion des usages licites a été très tôt identifiée comme la meilleure réponse au développement des usages illicites, un des facteurs du développement de ces derniers étant le coût de l'offre légale, qu'il s'agisse de l'achat des CD et DVD ou du téléchargement sur les sites ayant l'accord des ayants droit. Une charte d'engagements pour le développement de l'offre légale de musique en ligne, le respect de la propriété intellectuelle et la lutte contre la piraterie numérique avait été signée en juillet 2004 entre l'État, des sociétés de gestion collective, des syndicats professionnels et des fournisseurs d'accès ; elle prévoyait notamment l'engagement pour les ayants droit de « *développer la mise à disposition, dans des conditions, notamment financières, transparentes et non discriminatoires, sous réserve du secret des affaires et dans le cadre du droit de la concurrence, de l'intégralité des contenus numérisés et disponibles à l'ensemble des plates-formes, notamment celles qui seraient créées par les fournisseurs d'accès à internet* ». Une des missions de la HADOPI est d'encourager le développement de l'offre légale : à cette fin, elle attribue un label et a lancé un site recensant les offres culturelles labellisées par elle ou pouvant être regardées comme légales. Toutefois, la capacité des pouvoirs publics à jouer un rôle de prescription des comportements d'internautes grâce à ce type d'instruments reste sujette à interrogation[201].

La promotion de l'offre légale passe également par la levée d'obstacles réglementaires à la mise en ligne des contenus culturels, l'offre illicite n'étant par définition pas affectée par ces obstacles. En France, des réflexions ont été engagées à la suite du rapport Lescure sur la « *chronologie des médias* », un ensemble de règles législatives qui définissent le délai minimal séparant la sortie d'un film en

199. HADOPI, chiffres arrêtés à février 2014.

200. M. Imbert-Quaretta, *Rapport sur les moyens de lutte contre le streaming et le téléchargement direct illicites*, février 2013 ; M. Imbert-Quaretta et L. Dutheillet de Lamothe, *Outils opérationnels de prévention et de lutte contre la contrefaçon en ligne*, mai 2014.

201. Comme le reconnaît la HADOPI elle-même : « *À la lumière de l'expérience, le label – dans sa forme actuelle – s'avère limité pour faciliter l'identification des offres respectueuses des droits de propriété littéraire et artistique sur Internet* » (rapport d'activité 2012-2013, p. 8).

salles de ses différentes exploitations[202] ; les propositions formulées par le rapport Lescure et le CSA consistent à raccourcir le délai séparant la sortie d'un film et à réduire la période de « *gel des droits* », pendant laquelle les chaînes de télévision diffusant le film en ont l'exclusivité et empêchent la diffusion sur les plateformes de vidéo à la demande. Au sein de l'Union européenne, la Commission pousse à ce que les œuvres soient disponibles par-delà les frontières. En effet, la protection des droits d'auteur et droits voisins est accordée dans le cadre de chaque législation nationale et les sites qui proposent des œuvres culturelles en ligne doivent donc obtenir l'accord des organismes de gestion collective dans chaque pays. La directive n° 2014/26/UE du Parlement européen et du Conseil du 26 février 2014 concernant la gestion collective du droit d'auteur et des droits voisins et l'octroi de licences multiterritoriales de droits sur des œuvres musicales en vue de leur utilisation en ligne dans le marché intérieur poursuit ce but d'encouragement de l'octroi de licences valables simultanément dans plusieurs pays. Dans le même objectif, la Commission a engagé une consultation publique plus large sur une éventuelle réforme des règles du droit d'auteur, qui s'est achevée en mars 2014 et qui a recueilli plus de 11 000 contributions.

1.4. Internet n'échappe ni en fait, ni en droit à la puissance étatique, mais lui pose des défis inédits

L'évolution d'internet n'a pas confirmé les thèses selon lesquelles il échapperait à la puissance des États. Internet soulève cependant des difficultés spécifiques pour ceux-ci, tenant à son mode de gouvernance, à la détermination de la loi applicable et à l'effectivité de l'intervention juridique.

1.4.1. La théorie selon laquelle internet échappe ou devrait échapper à la puissance de l'État apparaît aujourd'hui démentie

Contrairement à ce qu'avaient espéré ses pionniers, internet n'est pas un espace hors du droit, régi par les usages émanant de la communauté de ses utilisateurs. Dans les débuts d'internet, l'*Internet Engineering Task Force*, une instance d'autorégulation des parties prenantes du réseau (cf. *infra*) avait défini en 1995 une « *Netiquette* », formalisée dans une recommandation (*Request for Comments*), qui définissait une série de règles de courtoisie et de bon usage dans la communication par messagerie électronique ou sur les forums. Sur un registre plus politique, la « *Déclaration d'indépendance du cyberespace* » du 8 février 1996[203] s'oppose de manière catégorique à l'intervention des États. Écrite en réaction au *Telecommunications Act*, la première loi à traiter explicitement d'internet aux États-Unis, sous la forme

202. Sous forme de vidéogramme – c'est-à-dire de DVD ou d'autres supports permettant la conservation d'un programme audiovisuel – dans le cadre d'un service de vidéo à la demande, à la télévision.

203. Dont l'auteur John Perry Barlow, activiste, fut l'un des fondateurs de l'*Electronic Frontier Foundation* (EFF), une ONG américaine spécialisée dans la défense des droits sur internet.

d'une exhortation aux « *gouvernements du monde industriel* », elle conteste tant la légitimité de la puissance publique à réglementer le cyberespace que sa capacité à le faire : « *Vous n'avez pas le droit moral de nous gouverner, pas plus que vous ne disposez de moyens de contrainte que nous ayons des raisons de craindre* ». Elle décrit internet comme un monde de pleine liberté (« *un monde où chacun, où qu'il soit, peut exprimer ses convictions, aussi singulières qu'elles puissent être* »), dont les règles sont définies de manière autonome par sa communauté (« *Nous croyons que c'est à travers l'éthique, l'intérêt individuel éclairé et le bien collectif, qu'émergera la conduite de notre communauté* »). Selon la formule de David Clark, un ingénieur du MIT qui fut l'un des principaux responsables de la conception de l'architecture du *net* dans les années 1980 : « *We reject : kings, presidents and voting. We believe in : rough consensus and running code* »[204].

Les deux postulats de cette approche libertaire, le défaut de légitimité des États à réglementer internet et leur incapacité à le faire, apparaissent aujourd'hui erronés. Les États ne sont pas moins légitimes à légiférer sur les réseaux numériques que sur tout autre pan des activités humaines, tout simplement parce que ce sont des activités humaines qui se déroulent sur ces réseaux : les internautes commercent, s'éduquent, écoutent de la musique, s'informent, opèrent sur des marchés financiers, font de la politique, travaillent ou jouent. L'idée d'un espace virtuel et immatériel, distinct de l'espace physique et réel, n'apparaît plus pertinente pour décrire internet, si elle l'a jamais été[205]. Selon Nathan Jurgenson, différentes évolutions (la reconnaissance faciale, la géolocalisation, l'internet des objets) tendent au contraire à une imbrication de plus en plus forte des activités en ligne et hors ligne[206]. La légitimité des États à encadrer les activités qui se déroulent sur internet n'est limitée que par le nécessaire respect des droits fondamentaux, en particulier la liberté d'expression.

La capacité des États à exercer leur pouvoir sur internet est elle aussi avérée. L'illustration la plus extrême en est donnée par les pratiques d'États non démocratiques, qui parviennent à entraver de manière significative l'accès de leurs ressortissants à internet, en utilisant diverses techniques : blocage d'adresses IP ou de noms de domaine, censure de certains mots-clés sur les moteurs de recherche ou filtrage des sites contenant ces mots-clés. Selon le rapporteur spécial des Nations unies sur la promotion et la protection du droit à la liberté d'opinion et d'expression, la pratique de blocages ciblés dans le temps, à des moments particuliers tels que des élections, des troubles ou la commémoration d'événements historiques, tend également à se développer[207].

---

204. « A Cloudy Crystal Ball. Visions for the Future », intervention devant l'IETF, juillet 1992.
205. L'idée d'immatérialité de l'internet est très présente dans la Déclaration d'indépendance du cyberespace pour justifier l'absence de légitimité des États : « *Vos notions juridiques de propriété, d'expression, d'identité, de mouvement et de circonstance ne s'appliquent pas à nous. Elles sont fondées sur la matière, et il n'y a pas de matière ici.* ».
206. N. Jurgenson, « Digital Dualism Versus Augmented Reality », *Cyborgology*, février 2011.
207. F. La Rue, *op. cit*.

Les États de droit exercent également, dans des cadres définis par la loi et sous le contrôle du juge, un pouvoir de contrainte sur internet. Des tribunaux ordonnent le déréférencement de certains sites, tranchent des différends sur des noms de domaine portant atteinte à des marques, enjoignent de publier une condamnation sur la page d'accueil d'un site. Les lois définissant le régime de responsabilité des intermédiaires techniques, le principe de limitation dans le temps de la conservation des données personnelles et les exceptions au droit d'auteur jouent un rôle structurant dans le fonctionnement de certains aspects d'internet. En imposant aux opérateurs de télécommunications et aux hébergeurs de conserver les données de connexion de leurs utilisateurs durant un an, notamment pour les besoins de la recherche, de la constatation et de la poursuite des infractions pénales, la loi fait de très nombreux acteurs de l'internet des auxiliaires potentiels de la justice.

1.4.2. Internet soulève cependant des difficultés quant à son mode de gouvernance, à la détermination de la loi applicable et à l'effectivité des interventions de l'État

Que la puissance de l'État parvienne à s'exercer sur internet ne signifie pas qu'elle n'y rencontre pas des difficultés particulières. Celles-ci tiennent notamment au mode de gouvernance d'internet, à la détermination de la loi applicable et à l'effectivité des interventions de l'État.

Un mode de gouvernance internationale dans lequel les États ne sont que des parties prenantes parmi d'autres

Au XIXe et au XXe siècle, plusieurs innovations technologiques ont suscité la création d'organisations intergouvernementales destinées à traiter des questions de coopération internationale qu'elles posaient. Ce fut le cas du téléphone, avec l'Union télégraphique internationale fondée en 1865, devenue l'Union internationale des télécommunications (UIT) en 1932 ; de la poste[208], avec l'Union postale universelle (UPU) en 1874 ; du chemin de fer, avec l'Union internationale des chemins de fer (UIC) en 1922[209] ; de l'aviation, avec l'Organisation de l'aviation civile internationale (OACI) en 1944. L'UIT et l'UPU sont les plus anciennes des organisations intergouvernementales ; le progrès technique, en renforçant l'interdépendance entre les États, a ainsi été un des moteurs de la coopération internationale.

Internet n'a pas suivi cette voie : il n'existe pas d'organisation intergouvernementale de l'internet. Deux facteurs y ont sans doute contribué. D'une part, un État particulier, les États-Unis, a joué dans la conception d'internet un rôle qui, s'il ne fut pas exclusif, a été sans conteste déterminant ; une telle configuration n'avait jamais existé dans de précédentes innovations technologiques. Internet a longtemps été directement géré par des entités de l'administration américaine, la DARPA et la *National Science*

208. La poste n'était certes pas une innovation technologique en 1874, mais le besoin de créer une organisation internationale était lié au développement des moyens de transport, qui accroissait de manière considérable le trafic postal international.

209. L'UIC est une association de droit privé, mais elle a été créée à l'initiative des États.

Foundation. En raison de l'essor d'internet, le gouvernement américain a abandonné cette gestion directe mais a souhaité jusqu'à ce jour maintenir une tutelle, qui se manifeste notamment par le fonctionnement de l'ICANN (cf. *infra*). D'autre part, la gouvernance d'internet reflète les modalités de travail de ses inventeurs, des ingénieurs informaticiens, habitués à définir les solutions techniques par la recherche d'un consensus au sein d'une communauté de sachants ; c'est la culture du « *rough consensus* », du consensus approximatif, dans laquelle une décision est prise lorsque toutes les objections sérieuses ont été levées, qui n'est pas transposable à la coopération intergouvernementale. La gouvernance d'internet a en grande partie été pensée comme le prolongement d'un travail technique sur un code informatique : les standards définis par l'une des entités impliquées dans cette gouvernance, l'IETF (cf. *infra*), sont toujours dénommés « *Request for Comments* » (RFC), maintenant l'expression employée pour la première fois par Steve Crocker en 1969 et figurant l'image d'un informaticien proposant son logiciel à la communauté pour recevoir des suggestions d'amélioration. Nombre des « *pères fondateurs* » de l'internet jouent d'ailleurs toujours un rôle déterminant dans ses instances de gouvernance : Steve Crocker est ainsi président du conseil d'administration de l'ICANN, tandis que Tim Berners-Lee dirige le *World Wide Web Consortium.*

Le terme de gouvernance est particulièrement approprié au sujet d'internet, puisqu'il n'existe pas d'autorité centrale mais une pluralité d'instances traitant de divers aspects de son fonctionnement. Elles peuvent être classées en trois catégories : l'instance chargée du système des noms de domaine ; les instances définissant les standards techniques d'internet ; les instances traitant de questions politiques, économiques et sociétales liées à internet.

• *La coordination du système des noms de domaine : l'ICANN*

Jusqu'en 1998, le système des noms de domaine, c'est-à-dire l'attribution des adresses IP et des noms de domaine correspondants, était géré sous la responsabilité directe du gouvernement américain. L'*Internet Corporation for Assigned Names and Numbers* (ICANN), organisation à but non lucratif de droit américain, assure depuis cette date la coordination du système. Elle décide de la création des extensions génériques de premier niveau (.com, .net, etc.)[210] et choisit leurs gestionnaires[211]. Les extensions nationales (.fr, .de, .uk, etc.) sont gérées sous la responsabilité des États, mais dans des conditions de dépendance technique à l'égard de l'ICANN, les décisions d'attributions des noms de domaine à extension nationale devant être référées aux « serveurs racine » gérés sous la responsabilité de l'ICANN. L'ICANN a pris au cours de son histoire des décisions structurantes sur le fonctionnement des noms de domaine, tels que l'autorisation de définir les noms de domaine dans des alphabets autres que l'alphabet latin (chinois, cyrillique, arabe,

210. Jusqu'en 2012, les extensions génériques de premier niveau étaient en nombre limité. L'ICANN a décidé de libéraliser ces extensions à compter de cette date, mais c'est-elle qui valide les candidatures pour la création de nouvelles extensions, selon des règles et une procédure qu'elle a définie.

211. La gestion du registre du .com, l'extension la plus utilisée, est ainsi assurée par la société *Verisign* dans le cadre d'un contrat avec l'ICANN.

etc.), la libéralisation des extensions génériques ou le passage de l'IPv4 à l'IPv6 (un nouveau mode de définition des adresses IP visant à répondre à la saturation de l'IPv4, dans lequel toutes les adresses possibles ont déjà été attribuées).

Les États-Unis maintiennent à ce jour une tutelle sur l'ICANN : celle-ci opère dans le cadre d'un contrat avec le département du commerce et la fonction technique de gestion du système s'opère toujours sous la supervision de la *National Telecommunications and Information Administration* (NTIA). Quant aux autres États, ils sont représentés auprès de l'ICANN dans un *Governmental Advisory Committee* (GAC), mais comme l'indique son nom, le rôle de ce comité n'est que consultatif.

• *La définition des standards techniques d'internet : l'IETF et le W3C*

Les standards techniques utilisés quotidiennement dans le fonctionnement d'internet émanent principalement de deux entités, *l'Internet Engineering Task Force* (IETF) et le *World Wide Web Consortium* (W3C). De manière schématique, l'IETF définit les standards utilisés dans la couche des communications, notamment ceux du protocole TCP/IP, tandis que le W3C travaille sur ceux de la couche des contenus, c'est-à-dire des langages utilisés pour définir le contenu des pages des sites internet (langage HTML, XML, etc.). L'IETF est aujourd'hui une entité de l'*Internet Society* (cf. *infra*), tandis que le W3C est un consortium d'organismes de recherche, dont les membres principaux sont le MIT, le consortium européen ERCIM[212], l'université japonaise Keio et l'université chinoise Beihang. Les modes de fonctionnement de ces deux instances présentent de fortes similitudes, avec des groupes de travail ouverts à tout participant et un processus itératif et de recherche de consensus pour l'adoption des standards. Bien qu'utilisés de manière systématique, ces standards d'internet n'ont pas de portée juridique contraignante ; ils sont une illustration de l'effectivité que peut avoir le droit souple[213].

• *Le traitement des questions politiques, économiques et sociétales liées à internet : l'Internet Society et le Forum pour la gouvernance d'internet*

L'*Internet Society*, organisation à but non lucratif de droit américain, a été créée en 1992 à l'initiative de pionniers d'internet, notamment Vinton Cerf et Bob Kahn. Outre sa fonction technique qu'elle exerce à travers l'IETF, l'*Internet Society* se donne une mission générale de promotion de l'universalité d'internet et de maintien de son caractère ouvert et décentralisé. Elle prend position sur des sujets de politique publique tels que la propriété intellectuelle, la sécurité d'internet, la neutralité d'internet ou l'accès du plus grand nombre à internet.

Le Forum pour la gouvernance d'internet (FGI) a été créé à la suite du Sommet mondial pour la société de l'information tenu en 2003 et 2005 à Genève puis à Tunis. Conformément aux conclusions du Sommet, il s'agit d'une instance multipartite dans laquelle sont représentées l'ensemble des parties prenantes (gouvernements, secteur privé, société civile et organisations intergouvernementales). Son mandat

212. *European Research Consortium for Informatics and Mathematics*. L'INRIA est membre de ce consortium pour la France.

213. Cf. Conseil d'État, *Le droit souple,* étude annuelle 2013.

est de discuter des questions de politique publique liées à internet et de faciliter le dialogue entre ces parties prenantes. Le rôle du FGI est toutefois limité par le fait qu'il se borne strictement à un rôle de forum, c'est-à-dire de lieu de discussion entre les acteurs qui ne produit pas de prise de position commune.

• *Un modèle multipartite en voie d'évolution*

Malgré le caractère empirique et composite de cette architecture, un modèle de la gouvernance d'internet peut être défini, qui se caractérise par l'implication d'une diversité de parties prenantes, la place prédominante du droit souple et, de fait, une influence américaine qui demeure forte bien que les groupes de travail de ces entités soient ouverts à tous. La Conférence mondiale des télécommunications de Dubaï, tenue par l'UIT en décembre 2012 en vue de réviser le règlement des télécommunications internationales, inchangé depuis 1988, a été l'occasion d'une nouvelle affirmation de ce modèle par opposition au modèle intergouvernemental. Le projet de nouveau règlement, qui étendait la compétence de l'UIT à certains aspects du fonctionnement d'internet, a fait l'objet d'une forte opposition des grands acteurs d'internet et n'a été finalement ratifié que par une minorité d'États, ne comprenant ni les États-Unis ni les États membres de l'Union européenne. Dans sa contribution au sommet de l'UIT, l'*Internet Society* soulignait le succès du modèle multipartite, qui a assuré le développement d'internet que l'on connaît, et les dangers de rigidification liés à un accord étatique[214].

La gouvernance d'internet ne se réduit cependant pas à l'activité de ces instances. Les législations et les traités adoptés par les États en matière de protection des données personnelles, de propriété intellectuelle ou de cybersécurité y jouent un rôle sans doute au moins aussi important. La spécificité d'internet tient moins à l'absence du droit dur émanant des États, en réalité très présent comme on l'a vu tout au long de cette première partie, qu'à l'absence d'organisation interétatique et de convention internationale au niveau mondial. La gouvernance d'internet pourrait être décrite comme le fruit de la superposition d'un droit souple à l'échelle mondiale et d'un droit dur à l'échelle nationale ou régionale pour l'Europe.

La gouvernance d'internet est en outre appelée à connaître des évolutions à court terme. En réaction aux révélations sur les pratiques de surveillance du gouvernement américain, les dirigeants de plusieurs entités impliquées dans la gouvernance, dont l'ICANN, l'IETF, l'*Internet Society* et le W3C, ont adopté le 7 octobre 2013 une « *déclaration de Montevideo* », dans laquelle ils ont « *exprimé leur vive préoccupation face à l'érosion de la confiance des internautes au niveau mondial* » et « *appelé à l'accélération de la mondialisation des fonctions (…) de l'ICANN vers un environnement dans lequel toutes les parties prenantes, y compris tous les gouvernements, participent sur un pied d'égalité* ». En mars 2014, les États-Unis ont annoncé qu'ils renonçaient à leur tutelle sur l'ICANN et lui demandaient de rechercher un nouveau cadre de gouvernance fondé sur le consensus entre toutes les parties prenantes ; en conséquence, ils ne renouvelleront pas le contrat avec l'ICANN à son échéance en septembre 2015. La conférence mondiale multipartite sur l'avenir

214. Internet Society Submission, *ITU World Conference on International Telecommunication Regulations* (WCIT-12).

de la gouvernance d'internet, dite *NetMundial*, qui s'est tenue à Sao Paulo les 23 et 24 avril 2014, a conclu au renforcement du Forum pour la gouvernance d'internet et à la nécessité de mettre d'ici septembre 2015 un nouveau cadre de supervision des fonctions assurées par l'ICANN.

Des difficultés sur la détermination de la loi applicable

En rendant accessibles aux internautes de chaque pays les contenus et les services proposés dans le monde entier, internet crée de très nombreux conflits entre les systèmes juridiques des différents États. L'affaire *LICRA et UEJF c/ Yahoo !*, relatif à la vente aux enchères d'objets nazis sur le site de ce moteur de recherche, l'a illustré avec éclat. Par une ordonnance du 22 mai 2000, le juge des référés du tribunal de grande instance de Paris a ordonné à *Yahoo ! Inc*., la société-mère enregistrée aux États-Unis, « *de prendre toutes mesures de nature à dissuader et à rendre impossible toute consultation par un internaute appelant de France des sites et services litigieux dont le titre et/ou le contenu portent atteinte à l'ordre public interne, spécialement le site de vente d'objets nazis* ». La société *Yahoo !* a alors saisi la justice américaine pour lui demander de déclarer cette sentence non exécutable aux États-Unis, au motif qu'elle serait contraire au 1er amendement de la constitution américaine. Si le juge de première instance lui a donné gain de cause, la cour d'appel fédérale compétente l'a déboutée à deux reprises[215]. Elle a notamment relevé que « *la France était en droit en tant que nation souveraine d'adopter des lois contre la distribution de propagande nazie, en réponse à sa terrible expérience des forces nazies durant la seconde guerre mondiale* » et que « *Yahoo ! ne pouvait s'attendre à bénéficier du fait que ses contenus puissent être vus dans le monde entier tout en étant protégée des coûts qui en résultent* »[216].

De manière curieuse et inexacte, cette affaire a parfois été comprise comme une illustration de l'impossibilité d'appliquer les lois françaises à une entreprise éditant un site internet de diffusion mondiale, notamment en raison de l'impossibilité technique de différencier le service proposé selon la nationalité des internautes. Comme l'avait déjà relevé le juge des référés du TGI de Paris, cette impossibilité technique n'existe pas : il est possible de déduire la nationalité des internautes de leur adresse IP. De multiples exemples plus récents témoignent de cette possibilité de différenciation. *Facebook* a renoncé en 2012 à proposer aux internautes européens son service « *Tag Suggest* » de reconnaissance faciale automatique sur les photos mises en ligne. Les sites qui diffusent de manière licite des contenus musicaux ou audiovisuels ne les proposent qu'aux internautes des pays dans lesquels ils ont recueilli l'accord des ayants droit. Le site de vidéo à la demande *Netflix* ouvre pays par pays. En outre, l'affaire *Yahoo !* atteste que les jugements d'une juridiction française peuvent être suivis d'effet : *Yahoo !* a modifié quelques mois après l'ordonnance sa politique sur la mise en ligne de contenus à caractère xénophobe, même si elle a prétendu que l'ordonnance n'était pas à l'origine de cette décision.

---

215. Cour d'appel fédérale du 9e circuit, 23/8/2004 et 12/1/2006, *LICRA and UEJF vs Yahoo !*, n° 01-17424.

216. Traduction des auteurs.

De nombreuses affaires ont depuis lors illustré la possibilité pour les juridictions d'un État de prononcer des décisions à l'encontre de sociétés établies dans d'autres États et exploitant des sites internet. Au cours de l'année 2013, le tribunal de grande instance de Paris a ainsi enjoint à plusieurs moteurs de recherche établis aux États-Unis de déréférencer des sites proposant de manière massive des contenus méconnaissant le droit de la propriété intellectuelle[217] ou des images portant atteinte à la vie privée d'une personnalité[218].

Cependant la fréquente confrontation de systèmes juridiques différents qu'occasionne internet est source d'une double difficulté pour les États : d'une part, la complexité des règles de droit international privé, qui déterminent la loi applicable et la juridiction compétente, est source d'incertitudes ; d'autre part, ces règles peuvent désigner des juridictions et des lois étrangères. L'État est ainsi confronté à la possibilité que ses lois sur la protection des données personnelles, la liberté d'expression ou la propriété intellectuelle ne soient en définitive pas applicables à toutes les situations qu'il entend régir.

D'assez nombreuses décisions ont été rendues ces dernières années par la Cour de justice de l'Union européenne et la Cour de cassation, qui clarifient les solutions applicables aux situations fréquemment rencontrées sur internet. De manière schématique (cf. les tableaux récapitulatifs *infra*), deux matières peuvent être distinguées : la matière pénale et quasi-délictuelle, où prévaut le critère de l'activité « *dirigée* » vers un pays ; la matière contractuelle, où prévaut la volonté des parties.

En matière pénale ou quasi-délictuelle, la configuration est souvent celle d'un site internet géré par une personne résidant à l'étranger et qui a commis des faits (contrefaçon, atteinte à la vie privée, contenus xénophobes, etc.) susceptibles de constituer une infraction à la loi française ou ayant causé un dommage à une personne résidant en France. Dès lors qu'un site internet est presque toujours visible depuis la France, la question qui se pose est de savoir si cette accessibilité suffit à fonder la compétence de la justice française et l'application de la loi nationale, ou s'il est nécessaire que le site ait « *dirigé* » son activité vers la France, ce qui s'apprécie selon un faisceau d'indices (langue et monnaie utilisées, terminaison du nom de domaine, publicités visibles par des internautes français, etc.). Après quelques hésitations, la jurisprudence s'est détournée du critère de la simple accessibilité, qui tend à la multiplication des juridictions compétentes, pour retenir le critère de l'activité dirigée, qui restreint la compétence des juridictions françaises. Ce critère est en outre prévu par la proposition de règlement relatif à la protection des données personnelles pour déterminer son champ d'application lorsque le responsable du traitement est établi en dehors de l'Union européenne[219].

---

217. Affaire *Allostreaming* précitée.

218. TGI Paris, 6 novembre 2013, *Max Mosley c/ Google Inc et Google France*, RG 11/07970.

219. Article 3.2 : « *Le présent règlement s'applique au traitement des données à caractère personnel appartenant à des personnes concernées ayant leur résidence sur le territoire l'Union, par un responsable du traitement qui n'est pas établi dans l'Union, lorsque les activités de traitement sont liées: a) à l'offre de biens ou de services à ces personnes concernées dans l'Union; ou b) à l'observation de leur comportement.* »

En matière contractuelle, les textes de l'Union européenne (règlement Bruxelles I *bis* du 12 décembre 2012 concernant la compétence judiciaire, la reconnaissance et l'exécution des décisions en matière civile et commerciale, règlement Rome I du 17 juin 2008 sur la loi applicable aux obligations contractuelles) font une grande place à la volonté des parties. La loi applicable est en principe la loi choisie par les parties et celles-ci ont la possibilité d'inscrire dans le contrat des clauses attributives de juridiction. Cette place reconnue à la volonté des parties a une grande importance pratique, dès lors que la plupart des grandes entreprises de l'internet sont établies aux États-Unis et inscrivent dans leurs conditions générales d'utilisation (CGU) des clauses de désignation de lois et de juridictions américaines. Toutefois, les règlements prévoient un certain nombre d'exceptions, notamment lorsque l'une des parties est un consommateur, c'est-à-dire un non professionnel ; il bénéficie alors de la possibilité de saisir la juridiction de son domicile et de l'application de sa loi nationale[220]. Quel que soit le type de contrat, les lois de police et les dispositions d'ordre public priment sur la loi choisie par les parties.

Matière pénale

Contrairement à la matière civile et commerciale, il n'y a pas de dissociation entre les règles de détermination de la juridiction compétente, d'une part, et de la loi applicable, d'autre part.

Le champ d'application de la loi pénale française est déterminé par les articles 113-2 à 113-13 du code pénal : il couvre notamment
- les infractions commises sur le territoire de la République, ce qui est le cas dès lors qu'un des faits constitutifs de l'infraction est commis sur ce territoire (article 113-2) ;
- les crimes et délits commis en dehors du territoire de la République, lorsque l'auteur ou la victime est de nationalité française, dans les conditions définies par les articles 113-6 et 113-7.

La principale question qui s'est posée à la jurisprudence est de savoir si le fait qu'un site accessible depuis la France offre un contenu en infraction avec le droit pénal français suffit à considérer que l'infraction a été commise sur le territoire. Dans un premier temps, les juridictions pénales ont considéré que l'accessibilité du site internet suffisait à fonder la compétence du juge français (TGI Paris, 3/11/1998, *UNADIF c/ Faurisson*, et Trib. Corr. Paris, 26/2/2002, *Yahoo !*). La Cour de cassation juge à l'inverse aujourd'hui que le site internet en cause doit être destiné au public français pour que le juge pénal soit compétent (Crim. 9/9/2008, *Giuliano F.*, n° 07-87.281).

La convention de Budapest sur la cybercriminalité prévoit que les États sont compétents lorsque l'infraction pénale a été commise sur leur territoire (article 22), mais elle ne précise pas comment doit être apprécié ce critère pour les infractions constituées par le contenu d'un site internet.

220. Le critère de l'activité dirigée resurgit pour déterminer le champ d'application de ces règles spécifiques : pour qu'une personne bénéficie de la protection reconnue aux consommateurs, il faut que le site ait dirigé son activité vers l'État de résidence de cette personne.

Matière civile et commerciale, litige relatif à des obligations non contractuelles

• Loi applicable

La loi applicable est celle choisie par les parties (article 3.1 du règlement Rome I). À défaut de choix, les contrats de vente de biens et de prestation de services sont régis par la loi du pays de résidence habituelle du vendeur ou du prestataire de services (article 4).

En matière de contrats conclus par les consommateurs, la loi applicable est celle du pays de résidence habituelle du consommateur, à condition que le professionnel exerce son activité professionnelle dans ce pays ou dirige son activité vers ce pays (article 6.1). Les parties peuvent convenir d'une autre loi, mais ce choix ne peut avoir pour résultat de priver le consommateur de la protection à laquelle il aurait eu droit en vertu de la loi de son pays de résidence (article 6.2).

La loi désignée en vertu du règlement Rome I ne peut porter atteinte à l'application d'une loi de police du juge saisi (article 9). En outre, l'application d'une disposition de la loi désignée par le règlement peut être écartée si elle est manifestement incompatible avec une disposition d'ordre public du juge saisi (article 21).

• Juridiction compétente

- Lorsque le défendeur est domicilié sur le territoire de l'Union européenne

La juridiction compétente est celle de l'État du défendeur. Toutefois, le plaignant peut aussi saisir la juridiction de son État de domicile lorsqu'il s'agit du lieu « *où le fait dommageable s'est produit ou risque de se produire* » (article 7.2 du règlement Bruxelles I *bis*), ce qui peut être à son choix soit le lieu où le dommage est survenu ou risque de survenir, soit le lieu où a eu lieu l'événement à l'origine du dommage.

Pour qu'un État soit considéré comme le lieu de réalisation d'un dommage au sens de cet article, il n'est pas nécessaire que le site internet à l'origine du dommage « dirige » son activité vers cet État (CJUE 3/10/2013, *Pinckney c/ Mediatech*)[221].

La notion d'État du lieu de réalisation du dommage est appréciée différemment selon les matières :

- En matière d'*atteinte aux droits de la personnalité* (notamment le droit à la vie privée et le droit à l'image), le plaignant peut saisir, au titre du lieu de la réalisation du dommage, la juridiction du lieu où il a le centre de ses intérêts, qui sera

221. Contra Com. 20/3/2012, *Sanofi-Aventis c/ Novo Nordisk*, 11-10600 : pour déterminer si la France est le lieu de réalisation d'un dommage au sens du règlement *Bruxelles I*, il ne suffit pas que le site à l'origine du dommage soit accessible depuis la France, il faut que ce site soit destiné à la France.

compétente pour connaître de l'intégralité du dommage, quel que soit l'État dans lequel il est survenu (CJUE, Gde Ch., 25 octobre 2011, *eDate Advertising*).

- En matière d'*atteinte à une marque*, le plaignant peut saisir l'État d'enregistrement de la marque (CJUE, 19 avril 2012, *Wintersteiger*).

- En matière de *violation des droits patrimoniaux d'auteur*, le plaignant peut saisir la juridiction de l'État qui garantit les droits d'auteur, mais n'est compétente que pour le dommage causé dans cet État (arrêt *Pinckney c/ Mediatech* précité).

- Lorsque le défendeur n'est pas domicilié sur le territoire de l'Union européenne

Article 46 du code de procédure civile : « *Le demandeur peut saisir à son choix, outre la juridiction du lieu où demeure le défendeur : (…) - en matière délictuelle, la juridiction du lieu du fait dommageable ou celle dans le ressort de laquelle le dommage a été subi ;* ».

Com. 3/5/2012, *eBay c/ Louis Vuitton* : pour que la France soit le lieu du fait dommageable au sens de cet article, il faut que le site internet à l'origine du dommage s'adresse directement au public de France.

Matière civile et commerciale
litige relatif à des obligations contractuelles

• Loi applicable

La loi applicable est celle choisie par les parties (article 3.1 du règlement Rome I). À défaut de choix, les contrats de vente de biens et de prestation de services sont régis par la loi du pays de résidence habituelle du vendeur ou du prestataire de services (article 4).

En matière de contrats conclus par les consommateurs, la loi applicable est celle du pays de résidence habituelle du consommateur, à condition que le professionnel exerce son activité professionnelle dans ce pays ou dirige son activité vers ce pays (article 6.1). Les parties peuvent convenir d'une autre loi, mais ce choix ne peut avoir pour résultat de priver le consommateur de la protection à laquelle il aurait eu droit en vertu de la loi de son pays de résidence (article 6.2).

La loi désignée en vertu du règlement Rome I ne peut porter atteinte à l'application d'une loi de police du juge saisi (article 9). En outre, l'application d'une disposition de la loi désignée par le règlement peut être écartée si elle est manifestement incompatible avec une disposition d'ordre public du juge saisi (article 21).

• Juridiction compétente

- Lorsque le défendeur est domicilié sur le territoire de l'Union européenne

La juridiction compétente est celle de l'État du défendeur. Toutefois, le plaignant peut aussi saisir la juridiction du « *lieu d'exécution de l'obligation qui sert de base à la demande* » (article 7.1 a) du règlement Bruxelles I *bis*. En cas de convention attributive de juridiction, la juridiction compétente est exclusivement celle choisie par les parties (article 25.1).

- Les règles déterminant la juridiction compétente en matière de contrats conclus par les consommateurs sont spécifiques, afin d'assurer la protection du consommateur. Le consommateur peut se prévaloir de ces règles spécifiques dès lors que le contrat a été conclu avec une personne qui « *dirige ses activités* » commerciales vers cet État (article 17.1 c)[222]).

CJUE, Gde Ch., 7 décembre 2010, *Pammer et Hotel Apenhof* : définit le faisceau d'indices à prendre en compte pour savoir si un site internet dirige ses activités vers un État membre[223].

La juridiction compétente est alors celle du domicile du consommateur. Les clauses attributives de juridiction ne peuvent y déroger que si elles sont postérieures au différend.

- Lorsque le défendeur n'est pas domicilié sur le territoire de l'Union européenne

Article 46 du code de procédure civile : « *Le demandeur peut saisir à son choix, outre la juridiction du lieu où demeure le défendeur : (…) en matière contractuelle, la juridiction du lieu de la livraison effective de la chose ou du lieu de l'exécution de la prestation de service ;* ».

À compter du 10 janvier 2015, date d'entrée en vigueur du règlement Bruxelles I *bis*, les règles de détermination de la compétence pour les contrats conclus par les consommateurs sont celles fixées par le règlement même lorsque le défendeur n'est pas domicilié sur le territoire de l'Union européenne.

222. À compter du 10 janvier 2015, date d'entrée en vigueur du règlement Bruxelles I *bis* qui se substitue au règlement Bruxelles I, cette règle sera également valable lors le défendeur n'est pas domicilié sur le territoire de l'Union européenne.

223. Extrait de l'arrêt : « *Les éléments suivants, dont la liste n'est pas exhaustive, sont susceptibles de constituer des indices permettant de considérer que l'activité du commerçant est dirigée vers l'État membre du domicile du consommateur, à savoir la nature internationale de l'activité, la mention d'itinéraires à partir d'autres États membres pour se rendre au lieu où le commerçant est établi, l'utilisation d'une langue ou d'une monnaie autres que la langue ou la monnaie habituellement utilisées dans l'État membre dans lequel est établi le commerçant avec la possibilité de réserver et de confirmer la réservation dans cette autre langue, la mention de coordonnées téléphoniques avec l'indication d'un préfixe international, l'engagement de dépenses dans un service de référencement sur Internet afin de faciliter aux consommateurs domiciliés dans d'autres États membres l'accès au site du commerçant ou à celui de son intermédiaire, l'utilisation d'un nom de domaine de premier niveau autre que celui de l'État*

Des problèmes d'effectivité des interventions de l'État

Internet pose enfin trois problèmes spécifiques pouvant amoindrir l'effectivité des interventions de l'État : la facilité de recréation d'un site internet ayant été convaincu d'activité illicite, la nécessité d'obtenir l'exécution de décisions administratives ou juridictionnelles par des États étrangers et le décalage entre la vitesse d'évolution de l'univers numérique et le temps des processus institutionnels.

Tout d'abord, un internaute ayant vu un contenu qu'il avait mis en ligne retiré par une plateforme au motif de son illicéité (par exemple, en raison de son caractère xénophobe ou de la méconnaissance de droits de propriété intellectuelle) peut le remettre en ligne sur une autre plateforme, voire sur la même plateforme mais à une autre adresse.

En deuxième lieu, même lorsqu'une juridiction est compétente à l'égard d'un site établi à l'étranger, l'exécution des mesures qu'elle a décidées peut impliquer la coopération d'autorités administratives ou judiciaires étrangères. En dehors de l'Union européenne, ceci implique pour les bénéficiaires de la décision d'en solliciter *l'exequatur* dans l'État étranger, procédure qui peut être lourde.

Enfin, les processus de décision des autorités administratives ou juridictionnelles ont une certaine durée. La procédure mettant en cause les abus de position dominante de *Google* a débuté il y a plus de trois ans devant la Commission européenne ; les services et même la stratégie économique de *Google* ont été modifiés entre temps. Si la procédure initiée en 2013 concernant le système d'exploitation *Android* prend les mêmes délais, la décision de la Commission risque d'intervenir alors que les enjeux de concurrence se seront déplacés de l'internet mobile vers l'internet des objets. Le tribunal de grande instance de Paris a mis deux ans pour statuer sur l'affaire *Allostreaming* ; entre temps, des contenus ont été visionnés des dizaines de millions de fois en méconnaissance des droits de propriété intellectuelle, et d'autres sites à caractère illicite ont été créés. Il est certes important de respecter les exigences du caractère contradictoire de la procédure et de recueillir le point de vue des parties prenantes. Il n'en existe pas moins un hiatus entre ces délais de procédure et la rapidité des évolutions de l'univers numérique.

1.5. Le numérique, un espace de libertés et un enjeu stratégique

Le droit du numérique, presque inexistant il y a quinze ans, a acquis en ce court laps de temps une extension que les développements qui précèdent ont permis de mesurer. De cette multitude d'évolutions, deux tendances peuvent être retenues qui déterminent la manière dont la protection des droits fondamentaux doit aujourd'hui être repensée : le numérique ouvre de nouveaux espaces aux libertés ; il est par là-même un enjeu stratégique.

---

membre où le commerçant est établi et la mention d'une clientèle internationale composée de clients domiciliés dans différents États membres. ».

1.5.1 Le numérique ouvre de nouveaux espaces aux libertés

En permettant à chacun d'être en réseau avec tous, en rendant possible la mise en données du monde, en démultipliant sans cesse la puissance de calcul et d'utilisation de ces données, le numérique a donné aux personnes, aux entreprises et aux associations des capacités nouvelles pour exercer leurs libertés. Pour employer le concept forgé par le prix Nobel d'économie Amartya Sen[224], le numérique accroît les « *capabilités* » des individus, c'est-à-dire leur capacité effective à jouir de leurs libertés, tant individuelles que collectives. Trois libertés l'illustrent particulièrement : la liberté d'expression (a), le droit à la vie privée (b) et la liberté d'association (c).

(a) L'ouverture de nouveaux espaces bénéficie manifestement à la liberté d'expression, dans ses deux dimensions définies par l'article 10 de la convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales : la liberté de « *recevoir ou de communiquer des informations* ». Du point de vue du récepteur, internet donne la capacité d'accéder de manière instantanée à tout contenu mis en ligne, quel que soit le lieu où réside son auteur ; si la convention a affirmé dès 1950 que la liberté d'expression devait s'exercer « *sans considération de frontière* », ce n'est que grâce à internet que les frontières ont été matériellement levées. Le saut franchi dans l'effectivité de la liberté d'expression est peut-être encore plus important du point de vue de l'émetteur : avant internet, le droit de communiquer ses pensées à autrui ne pouvait s'exercer au-delà d'un cercle limité de personnes que par l'accès à des médias (éditeurs, presse écrite, médias audiovisuels) jouant de manière inévitable un rôle de filtre ; aujourd'hui, chacun peut créer un blog, poster un commentaire, mettre en ligne une vidéo. Bien sûr, de nouveaux intermédiaires sont apparus (moteurs de recherche, plateformes de partage de contenus, réseaux sociaux) et sont devenus des prescripteurs incontournables en raison de la masse d'informations disponible sur le réseau ; l'importance de leur rôle soulève d'ailleurs des questions (cf. *infra* 2.3). Cependant, le filtre ne joue plus en amont, au stade de l'accès aux médias, mais en aval, au stade de la sélection des contenus par l'internaute lui-même. Il s'agit là d'un progrès considérable : si le nombre de contenus ayant une audience mondiale se comptant en dizaines ou en centaines de millions de lecteurs reste forcément limité, celui des contenus consultés par quelques centaines ou quelques milliers d'internautes s'est considérablement accru ; ce phénomène permis par le numérique est souvent qualifié de « *longue traîne* »[225]. Le *web* permet ainsi la diffusion d'une grande diversité de contenus à l'audience relativement faible mais qui peuvent toucher des communautés d'internautes rassemblés par une même langue, parfois rare[226], ou un même centre d'intérêt, parfois atypique. Somme toute,

224. Cf. notamment A. Sen, *L'idée de justice*, Flammarion, 2010.

225. Traduction de l'expression anglaise « *The long tail* », employée pour la première fois en 2004 par le rédacteur en chef du magazine *Wired* : C. Anderson, « The Long Tail », *Wired*, octobre 2004. L'expression s'inspire de la forme d'une courbe statistique décrivant la distribution des contenus en fonction de leur audience : à côté d'un petit nombre de contenus à forte audience, qui forment la bosse de la courbe, il y a un grand nombre de contenus à faible audience, qui forment la longue traîne.

226. L'encyclopédie *Wikipedia* contiendrait des articles dans près de 300 langues.

si comme l'affirme l'article 11 de la Déclaration de 1789, « *la libre communication des pensées et des opinions est un des droits les plus précieux de l'Homme : tout Citoyen peut donc parler, écrire, imprimer librement, sauf à répondre de l'abus de cette liberté dans les cas déterminés par la Loi* », alors internet est aujourd'hui l'un des instruments les plus précieux de l'un des droits de l'homme le plus précieux.

(b) S'agissant du droit à la vie privée, le numérique est souvent analysé comme une menace et présente en effet des risques réels (cf. *infra* 2.2) ; mais cela ne doit pas occulter sa contribution à l'épanouissement de la vie privée. Le droit à la vie privée n'est pas seulement le droit d'être protégé des immixtions d'autrui, mais aussi celui de nouer des relations personnelles avec les autres individus et de cultiver sa personnalité. En ce sens, la CEDH a jugé que « *le respect de la vie privée doit (…) englober, dans une certaine mesure, le droit pour l'individu de nouer et développer des relations avec ses semblables* » (16 décembre 1992, *Niemetz c. Allemagne*, n° 13710/88). De manière encore plus claire, l'article 2 de la Loi fondamentale de l'Allemagne dispose que « *chacun a droit au libre épanouissement de sa personnalité pourvu qu'il ne viole pas les droits d'autrui ni n'enfreigne l'ordre constitutionnel ou la loi morale*»[227]. Cette acception positive du droit à la vie privée, entendu comme un droit à l'épanouissement de sa personnalité, n'est pas exclusive de la conception négative du droit d'être protégé des immixtions d'autrui : il revient à l'individu de choisir dans quelle mesure il souhaite nouer des relations avec autrui et dans quelle mesure il souhaite en être protégé. Dans son acception positive, le droit à la vie privée bénéficie des nouvelles formes de sociabilité permises par les réseaux sociaux ou les messageries instantanées. Internet ouvre de nouvelles possibilités aux individus, par l'accès à l'information, aux produits culturels ou aux autres personnes partageant les mêmes centres d'intérêt, pour cultiver leurs goûts, faire de nouvelles rencontres et développer certains aspects de leur personnalité. Les pratiques de « *quantification de soi* » ou « *d'automesure* »[228], qui tendent à utiliser les données transmises par des applications ou des objets connectés pour améliorer la performance sportive, la productivité au travail ou encore la qualité du sommeil, renouvellent à leur manière l'aspiration ancienne à se connaître soi-même, en recourant aux outils contemporains de collecte, d'analyse et de visualisation des données[229].

---

227. Traduction en français donnée par le Bundestag : https://www.bundestag.de/htdocs_f/documents/cadre/loi_fondamentale.pdf

228. L'expression de « *Quantified Self* », que l'on peut traduire par « *quantification de soi* » ou « *automesure* », est issue d'un article de 2007 de Gary Wolf dans la revue *Wired*. Un mouvement international dédié à la promotion du *Quantified Self* a été créé la même année. Le « *chapitre* » français du *Quantified Self* a été créé en 2011 et en 2013, le quotidien gratuit *20minutes* a lancé le premier magazine en ligne dédié à l'automesure, intitulé *Se coacher.*

229. Les mêmes données peuvent être utiles à d'autres que la personne concernée et leur servir d'instruments de contrôle ; elles permettent par exemple à l'employeur de mesurer plus finement la productivité au travail de ses salariés. Les risques dont sont porteurs de telles utilisations par autrui sont examinés plus loin (cf. 2.2.1).

(c) Entendue strictement comme le droit de former « *la convention par laquelle deux ou plusieurs personnes mettent en commun, d'une façon permanente, leurs connaissances ou leur activité dans un but autre que de partager des bénéfices* », selon les termes de la loi du 1er juillet 1901, la liberté d'association n'a pas vu ses possibilités substantiellement étendues par le numérique, même si les associations peuvent bénéficier, comme d'autres entités, de la visibilité donnée par un site internet. En revanche, le numérique a ouvert un champ nouveau aux pratiques collaboratives et désintéressées, à travers les logiciels libres, l'élaboration collective de contenus (sites dits de type *Wiki*, à l'exemple de *Wikipedia*), le « *crowdsourcing* » ou encore les sites de partage (cf. *supra* 1.1.3). La diffusion « *virale* »[230] de l'information sur le *web* est un puissant levier pour les mobilisations collectives. Le numérique permet ainsi de faire vivre des collaborations désintéressées, que l'on pourrait qualifier « *d'associations informelles* », au-delà du cadre formel de l'association strictement entendue, les sites qui servent de cadre à ces pratiques étant d'ailleurs souvent portés par des structures juridiques à but non lucratif. Si ces associations informelles ne passent pas par un contrat d'association au sens juridique du terme, elles répondent à la même *affectio sociÉtatis*, la volonté d'agir en commun dans des buts non lucratifs.

1.5.2. Le numérique est un enjeu stratégique, qui suscite une vive compétition entre États et entre acteurs économiques

La contribution du numérique au développement économique est déterminante

La contribution du numérique à la croissance fait l'objet de controverses entre économistes. Dès 1987, le prix Nobel d'économie Robert Solow avait relevé qu'on « *voit les ordinateurs partout, sauf dans les statistiques de la productivité* » ; ce « *paradoxe de Solow* » continue de faire débat aujourd'hui, puisque la croissance des économies développées demeure plus faible qu'elle ne l'a été avant la diffusion des technologies numériques. Des économistes aussi respectés que Lawrence Summers[231] ou Robert Gordon[232] ont récemment affirmé que la croissance des pays industrialisés serait sans doute faible tout au long des prochaines décennies. Selon Robert Gordon, l'effet sur la productivité de la « *troisième révolution industrielle* » associée aux ordinateurs, à internet et aux téléphones mobiles n'aura été que de courte durée, entre la fin des années 1990 et 2004, et aura été bien moins durable et prononcé que celui de la deuxième révolution industrielle, liée à l'électricité et au moteur à combustion.

---

230. En permettant à chacun de partager un contenu avec tous ses contacts, qui eux-mêmes pourront le diffuser à tous les leurs, le *web* permet une diffusion extrêmement rapide ; elle est souvent qualifiée de « virale », à l'image de la propagation des virus biologiques.

231. Lors d'un discours prononcé au FMI le 8 novembre 2013, Lawrence Summers a employé la formule de « *secular stagnation* », que l'on peut traduire par « stagnation séculaire ».

232. R. J. Gordon, "Is U.S. Economic Growth Over? Faltering Innovation Confronts the Six Headwinds", *NBER Working Paper* n° 18315, août 2012.

En sens inverse, Erik Bryjnolfsson et Andrew McAfee[233], deux économistes du Massachussetts Institute of Technology (MIT), prédisent que les technologies numériques sont sur le point de provoquer une forte reprise de la croissance. Ils présentent deux arguments pour expliquer pourquoi la contribution du numérique au développement économique a jusqu'à présent été décevante. D'une part, les organisations mettent beaucoup de temps à s'adapter et à tirer parti d'une révolution technologique ; l'histoire économique conforte cette thèse, puisque l'apparition de l'électricité et de l'automobile ont d'abord coïncidé avec plusieurs décennies de faible croissance à la fin du XIXe siècle[234]. D'autre part, les progrès dans la puissance de calcul et le volume des données ayant un caractère exponentiel, leur rythme, trop lent au départ pour qu'il y ait un impact observable sur la croissance, va en s'accélérant[235].

Un autre thème de controverses tient à l'impact social du numérique, en termes d'emplois et d'inégalités. L'analyse économique a montré de longue date que le progrès technique pouvait être biaisé en défaveur des travailleurs non qualifiés ; il tend à faciliter l'automatisation de leurs emplois, alors qu'il accroît la demande de travailleurs qualifiés capables d'utiliser les nouvelles technologies. Dès 1981, Sherwin Rosen a parlé « *d'économie de superstars* »[236], dans laquelle « *le gagnant prend tout* » (« *winner takes all* »). Les évolutions récentes le confirment. Selon l'OCDE, le progrès technologique est la principale cause de la hausse des inégalités dans les pays développés au cours des trente dernières années, devant la mondialisation[237]. Les progrès de l'agilité des robots et de l'intelligence artificielle permettent de remplacer un nombre croissant d'emplois : selon deux économistes de l'université d'Oxford, 47 % des emplois seraient susceptibles d'automatisation dans les années à venir[238]. Le numérique crée par ailleurs de nombreux emplois, dans les domaines de la programmation, de l'analyse des données, du *design* ou de l'ingénierie ; mais les personnes dont les emplois sont détruits peuvent difficilement y accéder.

---

233. E. Bryjnolfsson et A. McAfee, *The Second Machine Age. Work, Progress and Prosperity in a Time of Brilliant Technologies,* W. W. Norton & Company, New York, 2014.

234. Dans le même sens, deux économistes français, Philippe Askénazy et Christian Gianella, ont montré qu'aux États-Unis, seules les entreprises qui avaient accompagné leur informatisation d'une réorganisation de leurs modes de production avaient enregistré une augmentation de leur productivité : cf. « Le paradoxe de la productivité : les changements organisationnels, facteur complémentaire à l'informatisation », *Economie et statistiques*, n° 339/340, 2000.

235. Pour illustrer cette idée, les auteurs racontent la légende de Sissa, l'inventeur indien du jeu d'échecs. Lorsque le roi Belkib l'interroge sur la récompense qu'il souhaite, il demande à recevoir un grain de riz pour la première case, deux grains pour la deuxième, quatre grains pour la troisième et ainsi de suite. Au départ surpris par ce qu'il croit être une demande très modeste, le roi ne se rend compte que cette demande va le ruiner qu'au milieu de l'échiquier. Pour les auteurs, nous sommes arrivés à ce point du « *milieu de l'échiquier* », où l'accélération des progrès liés au numérique va devenir manifeste.

236. S. Rosen, « The Economics of Superstars », *American Economic Review 71*, pp. 845-858.

237. OCDE, *Toujours plus d'inégalité : pourquoi les écarts se creusent*, avril 2012.

238. C. B. Frey et M. A. Osborne, *The Future of Employment : How Susceptible are Jobs to Computerisation*, Oxford University, septembre 2013.

Il n'entre pas dans l'objet de cette étude de trancher ces débats entre économistes. Force est cependant de constater que les plus récentes des évolutions décrites plus haut, telles que l'introduction du numérique dans un nombre croissant d'activités, la capacité nouvelle à utiliser les données et à en tirer de la valeur ainsi que les synergies apparaissant entre le numérique et d'autres innovations comme la robotique, semblent conforter la thèse de l'accélération développée par MM. Bryjnolfsson et McAfee ; le numérique ne se cantonne plus au commerce ou à la musique en ligne. En tout état de cause, il apparaît très probable qu'une part significative de la croissance future sera créée par le numérique, et que les pays dont l'économie numérique sera la plus dynamique bénéficieront de ce fait d'un avantage important. La contribution de l'économie numérique à la croissance est déjà nettement supérieure à sa part dans le PIB : en 2011, le cabinet McKinsey a ainsi estimé que ce qu'il qualifie de « *filière internet* », qu'il évalue à 3,7 % du PIB en 2010, contribuait à 25 % de la croissance française[239].

Ceci suffit à souligner l'intérêt général qui s'attache au développement de l'économie numérique. Quant à la progression des inégalités, si elle constitue un défi pour les politiques publiques, la limitation des progrès de l'économie numérique dans notre pays ne pourrait y apporter une réponse : du fait de l'internationalisation des échanges, elle conduirait seulement à ce que moins d'emplois soient créés sans ralentir les destructions.

Le numérique, espace de compétition et de rapports de forces

Les caractéristiques qui viennent d'être exposées – le fait que le numérique ouvre de nouveaux espaces de liberté et contribue de manière déterminante au développement économique – confèrent au numérique sa valeur. Si les usages du numérique se sont si vite développés, c'est parce qu'ils ouvrent aux individus de nouvelles possibilités de s'exprimer, de s'éduquer, d'accéder à la culture, de collaborer ou d'entreprendre. Si le numérique suscite l'intérêt croissant des États, c'est en raison de sa contribution potentielle à leur prospérité, à l'allongement de l'espérance de vie, à la sécurité ou à la maîtrise de leurs comptes publics. Le numérique crée de nouveaux territoires ; du fait de leur valeur, ils sont l'objet d'une vive compétition entre États et entre acteurs économiques :

- La concurrence entre entreprises est avivée par des caractéristiques propres à l'économie numérique. La course à la croissance y est particulièrement prégnante, en raison des effets de réseau (un réseau est d'autant plus attractif qu'il compte un grand nombre de membres) et de l'intérêt de détenir la plus grande quantité possible de données personnelles. Les frontières des « *marchés pertinents* », à l'intérieur desquels les biens et services sont substituables, ne sont pas stables : la concurrence classique entre acteurs d'un même marché se double d'une concurrence par la création de nouveaux marchés liés à la création de biens ou de services innovants.

239. McKinsey & Company, *Impact d'Internet sur l'économie française. Comment Internet transforme notre pays*, mai 2011.

Mus notamment par la volonté de recouper un nombre toujours plus important de données personnelles, les grands acteurs du numérique mènent des stratégies intenses de diversification[240] qui les conduisent à se concurrencer les uns les autres.

Les États voient dans le numérique des enjeux de compétition dans les domaines économiques, culturels et de sécurité. La dynamique de « *destruction créatrice* » des emplois, selon la formule de l'économiste autrichien Joseph Schumpeter, ne se fait pas forcément dans les mêmes proportions selon les États : les emplois créés dans un pays peuvent être détruits dans un autre, d'autant plus qu'internet permet la diffusion de services numériques partout dans le monde à un coût négligeable. Sur le plan culturel, en proposant partout dans le monde des services en apparence neutres (moteurs de recherche, sites de partage de contenus, services de numérisation des œuvres culturelles), les acteurs du numérique véhiculent néanmoins des valeurs (par exemple sur les limites souhaitables de la liberté d'expression), des systèmes juridiques (cf. *infra* 2.3.2 sur les questions de territorialité du droit) et, de manière inévitable, une certaine hiérarchisation des œuvres. En matière de sécurité, la maîtrise des technologies numériques et l'existence d'acteurs industriels puissants est susceptible de conférer des avantages décisifs dans la collecte de renseignement, comme l'ont illustré les révélations de l'ancien consultant de la NSA Edward Snowden, ou dans la capacité à perturber les systèmes informatiques d'un adversaire.

La place de l'Europe dans cette compétition suscite aujourd'hui l'inquiétude ; un rapport du Sénat se demande même si notre continent est en train de devenir une « *colonie du monde numérique* »[241]. Dans le classement des plus grandes entreprises mondiales du numérique, les compagnies européennes sont très peu nombreuses, distancées de manière écrasante par les firmes américaines mais aussi par les sociétés chinoises. Les Européens perdent des positions même dans le domaine de la téléphonie mobile, où ils devançaient les États-Unis au début des années 2000 ; *Nokia* a été racheté par *Microsoft* et l'Europe est en retard sur la Corée du sud dans l'accès au très haut débit. La part de la richesse consacrée par l'Europe à la recherche et au développement est nettement inférieure à ce qu'elle est aux États-Unis, au Japon ou en Corée du sud ; les marchés de capital-risque, qui jouent un rôle décisif dans l'amorçage des entreprises du numérique, sont bien moins développés sur notre continent qu'aux États-Unis. S'agissant en particulier

240. Partant de son moteur de recherche, *Google* a développé des dizaines de services allant de la messagerie personnelle à l'hébergement de fichiers et au réseau social. *Apple*, au départ fabricant de terminaux, est devenu un marchand de musique et une plateforme d'applications. *Amazon*, dont le cœur de métier était d'être un marchand en ligne, et *Microsoft*, éditeur de logiciels, se livrent aujourd'hui concurrence dans le domaine de l'informatique en nuage. *Apple*, *Google* et *Amazon* s'efforcent tous de se développer dans des domaines aussi variés que la télévision, la voiture connectées et les services de paiement.

241. Sénat, *L'Union européenne, colonie du monde numérique ?*, rapport fait au nom de la commission des affaires européennes par C. Morin-Desailly, mars 2013.

de la France, si certaines entreprises connaissent de réels succès[242], aucune n'est de taille mondiale ou en position de leader dans un secteur d'activité.

Outre sa faiblesse dans l'économie numérique, l'Europe témoigne d'une grande perméabilité aux services fournis par les Américains, plus importante que celle d'autres zones géographiques. *Google* y réalise des parts de marché supérieures à celles qu'il enregistre aux États-Unis. *Facebook* y est aussi largement dominant, alors qu'il est devancé par des sites locaux en Russie, au Japon ou en Corée du sud, sans parler de la Chine où il est encore largement interdit[243]. Les projets de services numériques européens peinent à se réaliser : s'il faut souligner la réalisation en cours de *Galileo*, dont l'objectif est de fournir une alternative au GPS, les tentatives de créer une bibliothèque numérique (*Europeana*) ou un moteur de recherche (*Quaero*) européens n'ont abouti que de manière incomplète. « *L'affaire Snowden* » a suscité des propositions en faveur d'un « *cloud européen* » destiné à assurer la sécurité des données personnelles et de celles des entreprises[244], mais celles-ci restent à concrétiser.

242. On peut par exemple mentionner la plateforme de partage de contenus *Dailymotion*, le site de musique en ligne *Deezer*, la société de marketing *Criteo*, l'hébergeur et prestataire d'informatique en nuage OVH ou encore les fabricants d'objets connectés *Withings* et *NÉtatmo*.

243. Interdit depuis 2009, de même que *Twitter*, *Facebook* n'a été réautorisé en septembre 2013 que dans une partie de Shanghai.

244. Cf. notamment en ce sens le relevé de conclusions du conseil des ministres franco-allemand du 19 février 2014.

L'ambivalence du numérique nécessite de repenser la protection des droits fondamentaux

Face à l'explosion numérique, le droit s'est déjà beaucoup transformé. Il n'est pourtant pas parvenu à un point d'équilibre. Les interrogations sur la pertinence du régime juridique des droits fondamentaux se succèdent au même rythme que celui des innovations dont le numérique est porteur. Réseaux sociaux, internet mobile, translation de l'audiovisuel vers internet, informatique en nuage, géolocalisation, reconnaissance faciale, *Big Data*, objets connectés, intelligence artificielle, robots : tous ces phénomènes, inexistants il y a encore quelques années, s'accompagnent de questions sur l'applicabilité de concepts juridiques élaborés avant leur apparition et sur l'effectivité des instruments dont dispose la puissance publique.

La difficulté d'y répondre tient à l'ambivalence intrinsèque du phénomène numérique. Le numérique ouvre de nouveaux espaces de libertés L'ambivalence du numérique est plus profonde que l'idée assez commune selon laquelle ce phénomène, comme d'autres technologies, peut avoir des usages bénéfiques ou néfastes. Le numérique n'est pas un outil docile pouvant être mis en œuvre selon la volonté de son maître, il induit des transformations qui échappent à la volonté de ses utilisateurs. Selon la terminologie du philosophe Bernard Stiegler, la technique n'est pas seulement constituée, elle est constituante ; selon celle de Lawrence Lessig, « *Code is Law* », formule qu'on peut traduire par « *le code informatique a force de loi* ». Cette ambivalence complique la tâche du législateur et du pouvoir réglementaire, car une intervention trop rigoureuse destinée à prévenir les aspects négatifs du numérique risque, du même mouvement, d'en entraver le potentiel positif.

Il n'y a pas là de fatalité : le code[245] peut être défini de façon à permettre le plein déploiement du potentiel de liberté recelé par le numérique, tout en limitant ses outils de surveillance à ce qui est strictement nécessaire pour la poursuite de finalités légitimes ; le droit est l'un des instruments qui y contribuent. Pour qu'il y parvienne, il faudra cependant repenser les modes de protection des droits fondamentaux, pour les adapter à l'explosion des données, au rôle inédit des grandes « plateformes » et au caractère transnational d'internet.

245. Que l'on peut entendre de manière large comme l'ensemble des éléments concourant à l'architecture des réseaux numériques, des terminaux et objets connectés aux infrastructures du réseau en passant par les services et contenus proposés sur ces réseaux.

La préservation du potentiel libérateur du numérique implique aujourd'hui trois réorientations : le droit à la protection des données personnelles doit être repensé, non dans ses principes mais dans ses modes de régulation (2.1) ; la liberté d'expression et la liberté d'entreprendre doivent être mieux garanties par une régulation limitant l'asymétrie entre les grandes plateformes et les autres acteurs (2.2) ; l'applicabilité des règles européennes aux internautes européens doit être mieux affirmée, tout en recherchant de nouveaux modes de coopération avec les autres espaces juridiques (2.3).

2.1. L'explosion des usages des données personnelles et des risques associés conduit à en repenser la protection

La première partie de cette étude a mis en évidence le rôle joué par les données personnelles dans les transformations associées au numérique. Grâce à la généralité de ses notions et à l'effort d'interprétation réalisé par la jurisprudence et le droit souple, le cadre juridique de la protection des données personnelles a pu continuer à être appliqué. De fortes interrogations sur ses principes et son effectivité se font cependant jour, qui appellent des réponses : le Conseil d'État estime que si les principes fondamentaux de ce cadre juridique conservent leur pertinence, les instruments de la protection des données personnelles doivent être profondément rénovés. Enfin, la surveillance exercée par les gouvernements, dont le principe est légitime mais dont l'ampleur potentielle a été récemment mise en lumière et portée à l'avant-scène du débat public, nécessite la mise en place de garanties spécifiques et renforcées.

Les contours de la notion de données personnelles faisant eux-mêmes débat, on adoptera d'emblée pour les besoins de l'exposé une approche large, avant de montrer (cf. *infra* 2.1.2) pourquoi cette approche large est, selon le Conseil d'État, justifiée.

2.1.1. L'explosion des usages des données personnelles est porteuse d'une augmentation des risques pour les personnes concernées

Une diversification des sources et de la nature des données personnelles en circulation

Au cours des premières décennies d'application de la loi du 6 janvier 1978, les données personnelles étaient recueillies par des entités organisées constituant des fichiers sur des individus dont elles avaient à connaître dans le cadre de leur activité. Les administrations publiques collectaient des données correspondant à leurs missions, pour alimenter des fichiers de sécurité sociale, des impôts, de police

ou de permis de construire. Les entreprises traitaient les informations concernant leurs salariés, leurs clients et leurs fournisseurs. Les associations constituaient des listes de leurs adhérents. Cette source de données que l'on peut qualifier d'institutionnelle perdure, mais trois autres sources sont venues la compléter :

- Il y a tout d'abord les données mises en ligne par les individus eux-mêmes. Dans le cadre des réseaux sociaux ou des sites de partage de contenus, les individus livrent sur eux-mêmes une grande quantité d'informations concernant leur situation familiale, leur activité professionnelle, leurs opinions, leurs centres d'intérêt ou leurs relations.

- Dans le même mouvement, les individus communiquent des informations sur des tierces personnes. L'exemple le plus typique est celui de la photographie partagée sur un réseau social, attestant que tel individu était tel jour dans tel lieu avec tel et tel autre individu, dans telle situation. L'accès et l'utilisation de ces photographies sont facilités par la possibilité d'y indiquer le nom des personnes qui y figurent (de les « *taguer* », selon l'expression consacrée), permettant par exemple à un moteur de recherche d'opérer le rapprochement entre la personne et les photos où elle figure. Il est même possible à un logiciel d'opérer la reconnaissance faciale automatique d'une personne en comparant une photographie à d'autres où elle est déjà identifiée[246].

- Enfin, les données personnelles sont de plus en plus fréquemment recueillies de manière automatique, selon divers procédés : installation de *cookies* sur le terminal de la personne concernée, envoi d'un signal de localisation à l'opérateur de télécommunications par un smartphone ou une tablette, recueil d'images par des caméras de vidéoprotection, etc. Le développement des objets connectés devrait amplifier cette collecte automatisée.

À cette diversification des sources s'ajoute une hétérogénéité accrue des données collectées. Les données recueillies par des institutions dans le cadre de fichiers sont structurées et correspondent le plus souvent à des caractéristiques objectives et relativement stables de l'individu telles que l'âge, le sexe, les revenus, la situation familiale ou les infractions commises. Les données disponibles aujourd'hui sur un individu sont disséminées, disparates et actualisables en permanence : il peut s'agir aussi bien de l'observation des goûts, des opinions, des relations, des lieux visités, des historiques de navigation sur internet, de photographies, de mentions de la personne sur un site internet, de messages échangés, de la vitesse d'une course à pied ou de tremblements corporels suggérant l'existence d'une maladie neurologique[247].

246. L'application développée à cette fin par *Facebook*, *Tag Suggest*, a été fermée aux internautes européens en 2012 à la demande des autorités du G29, mais reste accessible aux internautes américains.

247. Les accéléromètres et les gyroscopes présents aujourd'hui sur les smartphones permettent en effet de recueillir de telles informations.

Ce que les données personnelles disent de nous : le regard d'un psychanalyste

« *Le BFI, Big Five Inventory, est un inventaire de cinq grands types de personnalité auxquels sont corrélées des caractéristiques comme la performance au travail ou la capacité à prendre des décisions d'achat. Ce modèle distingue de nombreux aspects psychologiques comme l'ouverture à l'expérience, l'autodiscipline et le respect des obligations, l'énergie et la tendance à chercher la compagnie des autres, le goût de la coopération, ou au contraire le scepticisme, la tendance à la colère, à l'inquiétude ou à la dépression.*

Avec les simples données de mobilité de nos téléphones portables fournissant des indicateurs comme l'usage, la localisation, la régularité, la diversité des contacts, le temps mis à répondre à un texto, etc., il est aujourd'hui possible de prédire le résultat du test de n'importe quel abonné. Le modèle est relativement fiable, il est capable par exemple, à partir des données de mobilité, de prédire votre score d'extraversion d'une manière assez fidèle… (…)

Big Data *vous connaît mieux que vous ne vous connaîtrez jamais vous-même. C'est une mère monstrueuse, une Big Mother toute-puissante, celle qui a tout à la fois terrorisé et enchanté notre âme de nourrisson en comblant tous ses besoins, en anticipant tous ses désirs, en devinant ses pensées les plus secrètes, en dirigeant avec douceur et persuasion son existence dans ses moindres aspects, et pour son plus grand bien.* »

Extrait de Serge Hefez, « Big Mama », *Le un*, n° 10, 11 juin 2014.

Une logique économique qui pousse à la constitution d'ensembles de données toujours plus importants et riches d'informations

Si toutes ces informations restaient disséminées auprès des personnes qui les ont recueillies, les risques pour la vie privée seraient sans doute limités. La dynamique de l'économie numérique pousse cependant à leur regroupement.

Tout d'abord, certains acteurs sont en mesure[248], en raison de la nature du service qu'ils proposent, d'accéder par eux-mêmes, sans avoir à faire appel à des données collectées par d'autres, à une quantité considérable d'informations sur leurs clients. Pour certains acteurs, cette situation n'est pas nouvelle : depuis l'invention des cartes bancaires, les banques disposent d'une information détaillée, non seulement sur nos revenus mais aussi sur nos déplacements, nos achats et nos centres d'intérêt. Pour d'autres, le numérique l'a amplifiée : les opérateurs de télécommunications disposaient déjà de la liste de nos interlocuteurs, mais internet les a en outre informés des sites que nous visitions. Enfin, le numérique a suscité l'émergence d'acteurs entièrement nouveaux, tels les moteurs de recherche ou les réseaux sociaux, qui sont dépositaires, par leur fonction, de pans entiers de notre vie personnelle.

248. On traite ici des informations auxquelles leur activité leur donne potentiellement accès, sans s'intéresser à ce stade aux contraintes légales qui peuvent encadrer cet accès.

Ensuite, la valeur des données personnelles pousse à leur agrégation et à leur recoupement. La publicité joue à cet égard un rôle particulier : plus le nombre d'informations détenues sur le « profil » d'une personne est grand, plus les publicités qui lui sont adressées seront potentiellement pertinentes. La publicité comportementale, en particulier, repose sur le suivi de l'activité en ligne d'un individu ; la navigation sur des sites tout à fait différents est répertoriée par une société en mesure de le faire, soit parce qu'elle sert de régie publicitaire à ces différents sites, soit parce qu'elle y a inséré des possibilités d'interaction (boutons « j'aime » de *Facebook* ou « + 1 » de *Google*, boutons « partager » sur des réseaux sociaux, des plateformes de partage de contenus ou des messageries, etc.). Les possibilités de valorisation des données ne se limitent cependant pas à la publicité et couvrent l'ensemble des usages du *Big Data* : optimisation des processus de production, pilotage de la performance d'un service à partir des réactions des utilisateurs, personnalisation du service, etc. (cf. *supra* 1.1.1. et 1.1.2).

Deux catégories d'acteurs jouent un rôle particulier dans ces processus de recoupement des données personnelles. Il s'agit en premier lieu de fournisseurs de services aux consommateurs engagés dans des stratégies de diversification (a) ; en second lieu, d'intermédiaires spécialisés dans la collecte et la revente de données personnelles, moins connus du grand public mais dont le rôle est néanmoins considérable (b).

(a) Certains fournisseurs de services numériques aux consommateurs, dont le cœur de métier repose déjà sur une collecte massive de données personnelles, cherchent à amplifier encore cette collecte par la diversification des services proposés ou le rachat d'autres sociétés. Comme il a déjà été indiqué, *Google* a développé beaucoup d'autres services que son moteur de recherche (messagerie, cartes, traduction, hébergement de fichiers, partage de vidéos avec la société *Youtube* rachetée en 2006, etc.) qui lui apportent chacun certains types de données. Sa décision, prise en 2012, d'intégrer la soixantaine de règles de confidentialité correspondant à chacun de ces services en une politique unique, lui permettant ainsi de regrouper l'ensemble des données personnelles détenues sur chaque utilisateur, est à l'origine de la procédure coordonnée lancée à son encontre par le G29, qui a entraîné le prononcé de sanctions par plusieurs autorités de protection des données nationales[249]. De même, les rachats par *Facebook* des sites de partage de photographies *Instagram* et de messagerie instantanée *Whatsapp* sont en partie motivés par la volonté de compléter sa collecte de données personnelles. Les efforts de *Google*, d'*Amazon* ou de *PayPal* pour développer des offres de services de paiement au quotidien, dans le but de remplacer l'utilisation de la monnaie ou de la carte bancaire, visent à développer leur accès aux données relatives aux achats, riches d'information sur les centres d'intérêt de leurs clients et sur l'efficacité des publicités.

249. Le recours de *Google* contre la sanction de la CNIL est pendant devant le Conseil d'État à la date de rédaction de cette étude.

(b) Les « *data brokers* », expression que l'on peut traduire par « *courtiers en données personnelles* » ou « *revendeurs de données personnelles* », sont des acteurs spécialisés dans la collecte et la revente des données. Avant même l'essor du numérique, des listes de consommateurs étaient déjà vendues aux annonceurs, assorties de caractéristiques déduites d'indices tels que leur code postal ou de données publiques comme les fichiers de permis de construire ou de cartes grises. Le numérique a démultiplié leurs capacités de collecte de données personnelles et, ce faisant, transformé la nature de leur activité. Un rapport d'enquête de la commission du commerce du Sénat américain[250] a montré que les *data brokers* collectaient leurs données à partir de cinq sources principales : les fichiers gouvernementaux publics, l'achat de données (ou de licences d'utilisation de ces données) auprès d'autres sociétés, l'échange de données avec d'autres sociétés dans le cadre d'accords de coopération, les déclarations des consommateurs eux-mêmes dans le cadre d'enquêtes et de questionnaires[251] et les réseaux sociaux. Les données, le cas échéant enrichies par le *data broker* qui en infère d'autres caractéristiques des personnes concernées, sont ensuite revendues à d'autres acteurs, à des fins soit de marketing (les annonceurs cherchant à cibler leurs campagnes sur certains profils), soit d'évaluation de la personne avant un recrutement ou l'octroi d'un crédit ou d'une police d'assurance. L'ampleur des fichiers détenus par les *data brokers* est considérable : la société *Acxiom*, le leader du secteur, affirme ainsi détenir des données sur 700 millions de personnes dans l'ensemble du monde. Il n'existe pas à ce jour de travail d'enquête comparable sur l'activité des *data brokers* en Europe, où le cadre légal du traitement des données personnelles est sensiblement plus contraignant qu'aux États-Unis. Cette activité y apparaît cependant tout à fait significative, *Acxiom* revendiquant la détention de données relatives à 6 millions de foyers, avec 600 données en moyenne par foyer.

Au sein de la seconde catégorie, on peut identifier le sous-ensemble des « *annuaires en ligne* », dont l'activité consiste à proposer des services d'agrégation de l'ensemble des informations disponibles sur une personne sur internet[252]. C'est le cas par exemple des sites *Spokeo* ou *Rapleaf.* La société *Pages Jaunes* a également proposé un tel service entre 2010 et 2011, consistant dans l'affichage sur son service Pages Blanches des informations communiquées par le particulier sur plusieurs réseaux sociaux (*Facebook*, *Twitter*, *Copainsdavant*, etc.). De telles pratiques soulèvent des questions de conformité au cadre légal français de la

250. *A Review of the Data Broker Industry: Collection, Use, and Sale of Consumer Data for Marketing Purposes*, décembre 2013. L'enquête a porté sur les pratiques de neuf des principaux *data brokers* américains : A*cxiom, Experian, Epsilon, Reed Elsevier, Equifax, TransUnion, Rapleaf, Spokeo* et *Datalogix*.

251. La société Espsilon conduit ainsi une fois par an un « *Shopper's Voice Survey* », dans le cadre duquel les personnes contactées sont incitées à répondre par la possibilité de gagner des bons d'achat ainsi qu'un prix de 10 000 $ à l'issue d'un tirage au sort. Parmi les questions posées, elles sont invitées à dire si elles ou un membre de leur famille souffrent de problèmes cardiaques, de dépression, de troubles bipolaires ou de la maladie de Parkinson. 5,2 millions de personnes ont répondu à la dernière enquête.

252. Cette pratique de collecte automatisée à partir des pages *web* est parfois aussi dénommée selon l'expression anglaise de « *crawling* ».

protection des données personnelles. Par un arrêt du 12 mars 2014[253], le Conseil d'État a rejeté le recours formé par la société *Pages Jaunes* contre l'avertissement qui lui avait été adressé par la CNIL. Dans une autre affaire, la cour d'appel de Bordeaux a condamné au pénal, par un arrêt du 18 décembre 2013, une personne qui éditait plusieurs annuaires en ligne, notamment pour collecte de données personnelles par un moyen frauduleux, déloyal et illicite et pour traitement de données malgré l'opposition des personnes concernées.

Des partenariats entre ces différentes catégories d'acteurs peuvent amplifier encore l'agrégation des données. Ainsi, *Facebook* a conclu en 2013 un accord de partenariat avec plusieurs grands *data brokers* pour avoir accès par leur intermédiaire aux informations contenues dans les programmes de fidélité de nombreux commerçants. Ceci permet à *Facebook* d'accroître la pertinence de son ciblage publicitaire et de mieux en mesurer les résultats, les annonceurs pouvant être informés lorsque les personnes ayant vu leurs publicités effectuent par la suite des achats en magasin. De tels partenariats permettent de franchir la frontière entre les données sur l'activité des individus « en ligne » et « hors ligne », en l'occurrence les achats faits en magasin.

Des risques que les personnes concernées ne sont pas en mesure de maîtriser

Il est fréquemment relevé l'existence d'un « *paradoxe de la vie privée* »[254] : la plupart des individus se déclarent soucieux de la protection de leur vie privée et conscients que leur utilisation du numérique donne accès à un nombre considérable d'informations sur eux, mais prennent peu de mesures pour l'empêcher. Sans doute l'une des explications de ce paradoxe tient-elle à l'absence de vision claire de ce que pourraient être les conséquences négatives de cette dissémination d'informations personnelles. Il convient d'inventorier les risques qui y sont associés, avant de caractériser la situation née du cumul de ces risques.

• *Les différents risques associés à la diffusion des données personnelles*

Les risques décrits ci-dessous tiennent à des préjudices que la diffusion des données personnelles peut causer aux personnes concernées. Il convient de souligner, à titre préalable, que **la diffusion de données personnelles en dehors de la volonté de l'individu concerné** est en elle-même un risque, même si elle ne cause aucun préjudice.

---

253. CE 12 mars 2014, *Société Pages Jaunes Groupe*, n° 353193, à mentionner aux tables. Plusieurs motifs, constituant autant de violations de la loi du 6 janvier 1978, avaient été retenus par la CNIL dans son avertissement : déloyauté de la collecte des données et absence d'information des personnes quant à l'indexation de leurs profils sur les réseaux sociaux ; non-respect du principe de mise à jour des données ; non-respect des droits d'opposition et de rectification des personnes concernées ; non-respect de l'obligation de veiller à l'adéquation, à la pertinence et au caractère non excessif des données. Tous ces motifs ont été confirmés par la décision du Conseil d'État.

254. Cf. notamment S. Barnes, "A privacy paradox: Social networking in the United States", *First Monday*, Vol. 11, n° 9, septembre 2006.

Le premier risque de préjudice est le plus manifeste et peut paraître le plus anodin : il s'agit de **la réception de plus en plus fréquente de publicités de plus en plus ciblées et personnalisées**. La publicité personnalisée peut être bien perçue, comme apportant un service utile à son destinataire ou comme la contrepartie nécessaire d'un service gratuit ; mais elle peut aussi être vécue comme envahissante, soit par sa quantité, soit parce que la qualité même de son ciblage est ressentie comme intrusive. On pourrait donc parler d'un préjudice d'agacement. Certaines formes de publicité, qui utilisent le contenu de la messagerie personnelle[255], reposent sur des procédés de reconnaissance faciale[256] ou analysent les réactions corporelles de l'individu pour évaluer sa réception du message publicitaire, suscitent des controverses particulières. De manière générale, la part prise par la publicité dans le financement de l'économie numérique, phénomène que l'écrivain allemand Hans Magnus Enzensberger qualifie « *d'économie de la captation de l'attention* »[257], fait débat. Elle implique une marchandisation généralisée des données personnelles : les données d'un individu ont une plus grande valeur si celui-ci est très riche (bien que les données des pauvres puissent aussi avoir de la valeur, pour les raisons indiquées dans le paragraphe ci-dessous), atteint d'une maladie chronique ou sur le point d'avoir un enfant[258].

Le second risque, qui a trait également à l'utilisation commerciale des données personnelles, est celui de voir se développer **des pratiques commerciales abusives, consistant en une différenciation entre les clients à partir de l'exploitation de leurs données**. En elle-même, la différenciation des clients n'est pas condamnable, mais l'accès croissant des commerçants aux données personnelles, accroît le risque de pratiques abusives. La différenciation peut en premier lieu se faire par le marketing : d'après le calcul économique fait par l'annonceur, certains clients se verront proposer les offres les plus intéressantes, d'autres au contraire des propositions tirant parti de leur situation de faiblesse. Le rapport du Sénat américain a montré que les *data brokers* utilisaient les données collectées pour segmenter la population en catégories, l'intitulé de nombre de ces catégories se rapportant à la situation sociale difficile des intéressés, par exemple « *Rural and Barely Making It* », « *Ethnic Second-City Strugglers* » ou encore « *Tough Start: Young Single Parents* »[259]. Ces catégories désargentées s'avèrent être des cibles attractives pour les vendeurs d'un certain nombre de produits, notamment des crédits à la consommation à taux élevé. En second lieu, l'exploitation des données permet aux commerçants de différencier leurs prix et les autres caractéristiques

255. Ce qui est le cas de la messagerie *Gmail* de *Google*.

256. La chaîne britannique de supermarchés *Tesco* a ainsi lancé en novembre 2013 des écrans proposant aux clients passant devant eux des publicités personnalisées, définies en fonction des caractéristiques (âge, sexe) appréhendées à travers des procédés de reconnaissance faciale.

257. H. M. Enzensberger, « Le terrorisme publicitaire », *Le Monde*, 26 octobre 2013.

258. Le quotidien *Financial Times* propose sur son site un simulateur (« *How much is your personal data worth ?* »), permettant à chacun d'estimer la valeur de ses données personnelles, en fonction notamment de ces caractéristiques.

259. Respectivement « ruraux de condition modeste », « minorités ethniques de milieux urbains défavorisés » et « mauvais départ dans la vie : jeunes parents célibataires ».

de leurs offres en fonction des caractéristiques des clients, déplaçant ainsi à leur avantage l'équilibre de la relation entre client et vendeur. En effet, dans la relation classique, le vendeur ignore les préférences personnelles du consommateur et le prix qu'il est prêt à payer pour acheter tel bien ou service ; de plus, les possibilités de différencier les prix selon les consommateurs peuvent être limitées. Le numérique facilite tout à la fois la connaissance des préférences du consommateur, par l'exploitation de ses données, et la différenciation des prix, dans la mesure où l'internaute peut difficilement comparer le prix qui lui est proposé avec celui affiché aux autres consommateurs. Des pratiques dites « *d'IP tracking* », consistant pour les sites de voyage à reconnaître l'internaute grâce à son adresse IP et à lui proposer des prix plus élevés lorsqu'il consulte un trajet pour la seconde fois, ont ainsi été soupçonnées par le Parlement européen, même si la CNIL et la DGCCRF, dans une enquête sur plusieurs sociétés françaises conclue en janvier 2014, n'ont pas confirmé ces soupçons. En 2012, *Google* a obtenu un brevet aux États-Unis pour son système de « *dynamic pricing* », la description du brevet indiquant expressément que son objet est de permettre une différenciation des prix en fonction de la propension supposée du client à acheter tel ou tel contenu[260].

On peut qualifier de **risque de réputation** une troisième famille de risques, qui a trait à l'accès à l'assurance, au crédit, à l'emploi pour les salariés ou aux clients pour les professionnels. Dans tous ces domaines, des caractéristiques perçues comme défavorables peuvent conduire à en restreindre voire à en interdire l'accès. La dissémination des données personnelles accroît ces risques, soit que des informations se retrouvent sur internet et apparaissent dès que le nom de l'intéressé est mentionné sur un moteur de recherche, soit qu'elles figurent dans des bases de données auxquelles ont accès les acteurs concernés. Selon l'enquête du Sénat américain, les banques, les assureurs et les employeurs sont ainsi parmi les premiers acquéreurs des données détenues par les *data brokers* ; ils peuvent aussi s'intéresser aux données en ligne sur les réseaux sociaux. Dans certains cas, l'acteur observe directement dans les caractéristiques connues de l'individu un signal négatif, par exemple une mauvaise santé pour l'accès à l'assurance ou au crédit, ou un épisode professionnel antérieur défavorable pour l'accès à l'emploi. Dans d'autres cas, le signal négatif est déduit de corrélations statistiques : ainsi, dans le modèle de la société de crédit Zest Finance, les personnes qui saisissent leurs noms et prénoms uniquement en minuscules ou en majuscules, au lieu de respecter les règles d'orthographe, se voient attribuer un risque plus élevé[261].

De manière générale, la dissémination des données personnelles peut aussi alimenter toutes les formes de curiosité. Internet est ainsi devenu un instrument de travail obligé pour les « agences de recherche privées », que le code de la sécurité

260. United States Patent n° 8260657, http://patft.uspto.gov/netacgi/nph-Parser?Sect1=PTO1&Sect2=HITOFF&d=PALL&p=1&u=%2Fnetahtml%2FPTO%2Fsrchnum.htm&r=1&f=G&l=50&s1=8,260,657.PN.&OS=PN/8,260,657&RS=PN/8,260,657.

261. Exemple tiré de V. Mayer-Schönberger et K. Cukier, *Big Data. La révolution des données est en marche*, Robert Laffont, 2014. Le slogan de cette société (« *All Data is Credit Data* », qu'on peut traduire par « toute donnée personnelle peut servir à évaluer la solvabilité d'un emprunteur ») est éloquent.

intérieure définit comme « *la profession libérale qui consiste, pour une personne, à recueillir, même sans faire état de sa qualité ni révéler l'objet de sa mission, des informations ou renseignements destinés à des tiers, en vue de la défense de leurs intérêts* »[262].

La quatrième famille de risques a trait aux **utilisations malveillantes, portant directement atteinte aux biens ou aux personnes**. La dissémination des données personnelles accroît la probabilité qu'elles tombent entre de mauvaises mains, notamment à la suite de « *failles de sécurité* » chez les responsables de leur traitement. Ces informations peuvent ensuite être revendues, y compris à des acteurs ayant une activité licite mais peu regardants sur l'origine des données qu'ils traitent, donner lieu à un chantage à la divulgation lorsqu'elles ont un caractère sensible, ou servir à une usurpation d'identité. Selon un sondage réalisé par l'institut CSA en 2012, 8 % des Français déclaraient avoir été victimes d'une usurpation d'identité, contre 4 % trois ans plus tôt[263]. Aux États-Unis, le *data broker Experian* a vendu pendant un an des données personnelles à une entité spécialisée dans l'usurpation d'identité basée au Vietnam, dont le responsable s'était fait passer pour un détective privé ; il aurait ainsi eu accès aux données de 200 millions d'Américains[264].

Enfin, des risques spécifiques sont associés **à l'utilisation des données personnelles par les pouvoirs publics à des fins de sauvegarde de l'ordre public et de la sécurité nationale** ; ils seront examinés plus loin (cf. *infra* 2.2.5).

• *Une perte générale de maîtrise de leurs données par les individus, pouvant fragiliser la confiance dans les services numériques et porter atteinte aux libertés*

Le cumul de ces risques conduit à une situation que l'on peut qualifier de perte générale de la maîtrise de leurs données par les individus. La circulation des données se produit sans égard pour le contexte dans lequel elles ont été initialement obtenues : la donnée personnelle est traitée comme une marchandise et, comme telle, elle circule de main en main. Si les données concernant chaque individu restaient dispersées, elles ne présenteraient pas un grand risque, mais la société numérique se caractérise aussi par la capacité à les réagréger, à travers des outils comme les moteurs de recherche pour les données accessibles en ligne et des collecteurs tels que les *data brokers* pour celles qui ne le sont pas. À l'image d'un boomerang, la donnée personnelle laissée par un individu et qui a circulé bien loin de son utilisation initiale peut revenir vers lui, sans qu'il en ait forcément conscience, sous la forme d'une publicité ciblée, du refus d'un employeur de le recruter, d'une usurpation d'identité ou de la surveillance exercée par une agence de renseignement.

---

262. Cf. « Facebook, le meilleur ami du détective privé », *Libération*, 9 mars 2009.

263. « Les Français et la criminalité identitaire », sondage de l'institut CSA, octobre 2012.

264. Le jugement du responsable de cette entité, un Vietnamien âgé de 24 ans, est en cours dans le cadre d'une procédure de plaider-coupable. Cf. "Experian Lapse Allowed ID Theft Service Access to 200 Million Consumer Records", KrebsonSecurity, mars 2014, http://krebsonsecurity.com/2014/03/experian-lapse-allowed-id-theft-service-to-access-200-million-consumer-records/.

Le public est sans doute aujourd'hui au milieu du gué dans sa prise de conscience de cette situation : il comprend que le boomerang est lancé, c'est-à-dire que nombre des activités faites en ligne ou hors ligne laissent aujourd'hui des traces qui peuvent être réutilisées ; mais il ne perçoit pas encore bien comment le boomerang peut revenir vers lui, c'est-à-dire comment cette réutilisation peut se faire à son détriment. Cette compréhension incomplète explique le « *paradoxe de la vie privée* » : une inquiétude diffuse existe sur la dissémination des données personnelles, mais cette crainte n'a pas de réel objet, faute de mesure des risques tangibles. La prise de conscience du public se développe cependant. Les révélations concernant les pratiques de la NSA et d'autres services de renseignement ont ainsi fait évoluer l'opinion, notamment dans la compréhension des liens existant entre la collecte de données par des acteurs privés et leur réutilisation à des fins de protection de la sécurité nationale. La faille de sécurité dite « *Heartbleed* », découverte en avril 2014, pourrait jouer en raison de son ampleur un rôle similaire concernant les risques de réutilisation malveillante[265]. La réglementation peut également contribuer à la perception des menaces par les utilisateurs : l'obligation imposée aux opérateurs de communications électroniques d'informer les personnes concernées des « *violations de données à caractère personnel* », imposée par une ordonnance du 24 août 2011 et que la proposition de règlement relatif à la protection des données prévoit d'étendre à l'ensemble des responsables de traitement, devrait jouer en ce sens.

Il est souhaitable que le public perçoive mieux les risques associés à la société numérique ; un apprentissage est en cours, ce qui est naturel pour des usages encore très récents. Les comportements évoluent vite, comme en témoigne le succès de « *messageries éphémères* » comme *Snapchat*, où les messages et photos envoyés disparaissent en quelques secondes, ou de réseaux sociaux alternatifs comme *Whisper* ou *Secret*, dont les utilisateurs sont anonymes ; ce succès s'explique en partie par la volonté des utilisateurs de jouir d'une liberté d'expression renforcée par l'absence de crainte de réutilisation[266].

Cependant, les progrès de la vigilance des utilisateurs ne doivent pas dégénérer en autocensure dans l'exercice des libertés. Il faut à cet égard souligner que le droit à la vie privée, en protégeant les individus dans leurs intérêts particuliers, est aussi une institution collective permettant l'exercice d'autres libertés, car il prémunit les citoyens de la crainte de la surveillance. Les Américains se souviennent que

---

265. Il s'agit d'une faille dans le logiel *OpenSSL*, utilisé par de très nombreux sites internet et pour des applications de messagerie afin de crypter les données échangées ; deux serveurs internet sur trois seraient concernés. La faille, qui a affecté le logiciel durant deux ans, permet notamment à des pirates d'accéder aux mots de passe des utilisateurs de ces sites.

266. Le fondateur et PDG de *Snapchat*, Evan Spiegel, présente son application comme permettant une expérience plus proche de la conversation dans la vie réelle : «*That's what Snapchat is all about. (…) Identity tied to now, today. Room for growth, emotional risk, expression, mistakes, room for you*" (cf. "The Secrets To Snapchat's Success: Connectivity, Easy Media Creation, And Ephemerality", *TechCrunch*, 25 janvier 2014, http://techcrunch.com/2014/01/25/how-snapchat-thinks-about-snapchat/.

leur service postal, dont Benjamin Franklin fut le premier directeur en 1775, a très tôt respecté le secret des correspondances en vertu du *Post Office Act* de 1792 ; pour les pères fondateurs des États-Unis, ce secret était une condition des libertés affirmées par la Déclaration d'indépendance et cette importance dans le fonctionnement de la démocratie américaine a été relevée par A. de Tocqueville. À la même époque, l'Assemblée constituante française, inspirée par les mêmes idéaux, affirmait le même principe par deux lois du 29 août 1790 et du 20 juillet 1791 ; de cette période date le « *serment du postier* »[267]. Le Conseil d'État a jugé que le secret des correspondances était une liberté fondamentale au sens du référé-liberté, dans une affaire où était en cause la liberté d'exercice par les élus de leur mandat[268]. À l'ère numérique, la dissémination des données personnelles et la facilité de leur recoupement ne sont pas moins susceptibles de porter atteinte aux libertés que ne le fut l'indiscrétion du fonctionnaire des postes.

Le schéma ci-dessous présente de manière synoptique les facteurs de perte de la maîtrise des données personnelles et les risques qui s'ensuivent.

Source : Conseil d'État, section du rapport et des études

267. Aujourd'hui prévu par le décret n°93-1229 du 10 novembre 1993 relatif au serment professionnel prêté par les personnels de *La Poste*.

268. CE, 9 avril 2004, *M. X*, n° 263759 au recueil. Dans cette affaire, le directeur général des services d'une collectivité territoriale avait ordonné aux agents d'ouvrir systématiquement le courrier destiné aux élus.

2.1.2. Le cadre de la protection des données personnelles demeure pertinent dans ses principes

Des interrogations sur les principes mêmes de la protection

Les interrogations portent sur le champ couvert par la notion de donnée à caractère personnel, sur les principes relatifs à la qualité des données issus de la convention n° 108 du Conseil de l'Europe et repris par la directive n° 95/46/CE, sur le rôle du consentement et du droit d'information et sur la notion de données sensibles.

• *Le champ couvert par la notion de donnée personnelle*

Selon l'article 2 de la directive, une donnée à caractère personnel est une « *information concernant une personne physique identifiée ou identifiable* » ; il ajoute qu'est « *réputée identifiable une personne qui peut être identifiée, directement ou indirectement, notamment par référence à un numéro d'identification ou à un ou plusieurs éléments spécifiques, propres à son identité physique, physiologique, psychique, économique, culturelle ou sociale* ». Le considérant 26 précise que « *pour déterminer si une personne est identifiable, il convient de considérer l'ensemble des moyens* ***susceptibles d'être raisonnablement mis en œuvre****, soit par le responsable du traitement, soit par une autre personne, pour identifier ladite personne* ». L'article 2 de la loi du 6 janvier 1978 retient une approche plus large : il dispose que pour déterminer si une personne est identifiable, « *il convient de considérer* ***l'ensemble des moyens en vue de permettre son identification*** *dont dispose ou auxquels peut avoir accès le responsable du traitement ou toute autre personne* ».

Ces définitions donnent lieu à plusieurs incertitudes sur le champ d'application du cadre juridique de la protection des données personnelles, d'autant plus embarrassantes qu'elles concernent des pans entiers du fonctionnement des réseaux et de l'économie numérique. Les controverses portent notamment sur le statut de l'adresse IP, sur le régime applicable à la publicité comportementale et sur celui des pratiques relevant du *Big Data*.

Tout utilisateur d'un terminal connecté à internet se voit attribuer par son fournisseur d'accès une adresse IP, qui permet de l'identifier sur le réseau. Cette adresse est répertoriée par nombre d'acteurs, notamment les sites internet visités par cette personne. Dès 2000, le G29 a adopté un avis selon lequel l'adresse IP était une donnée personnelle au sens de la directive 95/46/CE, dès lors que les fournisseurs d'accès ou les gestionnaires de réseaux locaux (par exemple, ceux administrés par une entreprise) peuvent retrouver la personne qui l'a utilisée[269]. La Cour de justice de l'Union européenne a confirmé cette position, de manière implicite dans l'arrêt *Promusicae c/ Telefonica* du 29 janvier 2008 (Gde Ch., C-275/06), puis plus explicite dans l'arrêt *Scarlet c/ SABAM* du 24 novembre 2011 (C-70/10), où elle a relevé que les adresses IP étaient « *des données protégées à*

269. Le G29 a écarté l'objection selon laquelle il n'est pas toujours possible d'identifier l'utilisateur d'une adresse IP, notamment dans les cybercafés. Selon lui, dès lors qu'il n'est pas possible de distinguer *a priori* ces adresses collectives des adresses dont l'utilisateur est identifiable, l'ensemble des adresses IP doivent être regardées comme des données personnelles.

caractère personnel, car elles permettent l'identification précise [des] utilisateurs » (§ 51). Pourtant, ces prises de position ne semblent pas avoir mis fin au débat. Le débat juridique français, du moins, reste ouvert du fait des deux arrêts rendus par la cour d'appel de Paris le 27 avril et le 15 mai 2007 ; la cour y a jugé que « *cette série de chiffres (…) ne constitue en rien une donnée indirectement nominative relative à la personne dans la mesure où elle ne se rapporte qu'à une machine, et non à l'individu qui utilise l'ordinateur pour se livrer à la contrefaçon* ». Une proposition de loi votée par le Sénat le 23 mars 2010 a cherché à trancher le débat en disposant explicitement que les adresses IP étaient des données personnelles[270]. Mais elle n'a pas été définitivement adoptée par le Parlement et, en dépit des prises de position du G29 et de la CJUE, plusieurs des personnes auditionnées dans le cadre de cette étude ont estimé qu'il existait encore des incertitudes sur le statut de l'adresse IP.

S'agissant de la publicité comportementale, il est souvent affirmé que les données traitées ne sont pas des données à caractère personnel ; l'argument employé est que la régie publicitaire ne connaît pas l'identité de la personne qui visite le site, mais seulement un « *profil* », comportant des caractéristiques (âge, sexe, localisation géographique, etc.) qui vont susciter l'envoi de la publicité. Ainsi, le site www.youronlinechoices.eu, mis en œuvre par des fédérations professionnelles d'acteurs de la publicité[271] dans le cadre d'une recommandation de bonnes pratiques, indique que « *dans la plupart des cas, l'information utilisée pour vous communiquer des publicités n'a pas de caractère personnel, dès lors qu'elle ne vous identifie pas* »[272]. Dans un avis du 22 juin 2010[273], le G29 a adopté une position différente, en se fondant sur deux arguments : la publicité comportementale reposant sur le « *traçage* » du comportement d'un individu en ligne, à travers la reconnaissance de son adresse IP ou l'installation d'un cookie servant à l'identifier de manière unique, c'est donc bien un individu particulier qui est ciblé, même si son nom n'est pas connu de la régie ; l'information collectée par la régie a trait aux caractéristiques de la personne et a pour but de l'influencer par l'envoi de publicités adaptées. Dans ses réactions à la proposition de règlement relatif à la protection des données personnelles[274], l'*Internet Advertising Bureau*, qui regroupe les principaux acteurs de la publicité en ligne, continue d'affirmer que la collecte de données liée à un identifiant tel qu'un cookie ne devrait pas entrer dans le champ d'application des règles relatives à la protection des données à caractère personnel, dès lors que les opérateurs de ces *cookies* n'ont pas connaissance du nom de la personne.

---

270. Proposition de loi de M. Yves Détraigne et de Mme Anne-Marie Escoffier.

271. Notamment l'Alliance européenne pour l'éthique en publicité (*European Advertising Standards Alliance* ou EASA) et *l'Internet Advertising Bureau* (IAB).

272. "*in most cases the information used for providing you with these adverts is not personal, in that it does not identify you…*".

273. Article 29 Data Protection Working Party, "Opinion 2/2010 on online behavioural advertising", juin 2010, WP 171.

274. Cf. par exemple *IAB UK, House of Commons Justice Select Committee Inquiry into EU Data Protection Framework Proposals, Written Evidence from IAB UK*.

La question de l'applicabilité du cadre juridique de la protection des données à caractère personnel aux pratiques relevant du *Big Data* est également posée. Dans un grand nombre de cas, les données utilisées sont extraites de données à caractère personnel sans pour autant comporter le nom des individus : il en va ainsi des données sur le transport des passagers collectées par les passes *Navigo* de la RATP, de celles qui seront produites par les compteurs communicants mis en place par ERDF et GRDF ou encore des « *tweets* » écrits par les utilisateurs de *Twitter* et qui servent à analyser l'état de l'opinion. Les acteurs qui procèdent à l'utilisation de ces données peuvent arguer qu'ils ne sont pas intéressés par les caractéristiques de telle ou telle personne, mais par leur exploitation statistique, qui ne présente pas de risque d'atteinte à la vie privée. Cependant, la définition des données à caractère personnel par la directive n° 95/46/CE et *a fortiori* par la loi du 6 janvier 1978 est large : dès lors que l'individu auquel se rattache la donnée est identifiable, il s'agit d'une donnée à caractère personnel. Or, les évolutions récentes de la recherche statistique conduisent à envisager de manière plus large les possibilités de réidentifier une personne à partir de données anonymisées. Ainsi, une chercheure de Harvard, Latanya Sweeney, a montré que 87 % des Américains pouvaient être identifiés à partir de la seule combinaison de leur code postal, de leur date de naissance et de leur genre[275]. Paul Ohm, de l'université du Colorado[276], conteste de manière plus radicale la fiabilité de toute méthode d'anonymisation, sauf à retirer tout intérêt aux données traitées en raison de l'appauvrissement requis pour obtenir une anonymisation fiable[277].

• *Les principes relatifs à la qualité des données*

Les « *principes relatifs à la qualité des données* » sont au frontispice de la protection des données à caractère personnel. Prévus tant par l'article 5 de la convention n° 108 du Conseil de l'Europe que par l'article 6 de la directive n° 95/46/CE et de la loi du 6 janvier 1978, ils comportent l'obligation de loyauté, de collecte pour des finalités déterminées, explicites et légitimes, le principe de proportionnalité des données collectées à ces finalités, le principe d'exactitude et enfin la limitation de la durée de conservation. Le principe selon lequel les données à caractère personnel ne peuvent être traitées que pour des finalités déterminées est même prévu par l'article 8 de la Charte des droits fondamentaux de l'Union européenne, et figure donc au sommet de la hiérarchie des normes de l'Union. Ces principes sont pourtant contestés, au motif qu'ils entraveraient le développement du *Big Data*.

Les critiques mettent en avant le fait que la valeur créée par le *Big Data* repose sur la réutilisation des données à des fins qui n'avaient pas été prévues lors de leur collecte. Les auteurs du livre *Big Data. La révolution des données est en marche*[278]

275. L. Sweeney, "Simple Demographics Often Identify People Uniquely", Carnegie Mellon University, *Data Privacy Working Paper* 3, Pittsburgh 2000.

276. P. Ohm, "Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization", 57 *UCLA Law Review* 1701 (2010).

277. L'anonymisation est en effet opérée par la suppression des données susceptibles de permettre la réidentification de la personne ou par leur « *floutage* » (le code postal est remplacé par le département, la date de naissance par l'année de naissance, etc.).

278. V. Mayer-Schönberger et K. Cukier, o*p. cit*.

donnent ainsi l'exemple d'une entreprise ayant conçu un système d'antivol de voitures reposant sur un dispositif biométrique de reconnaissance des points de pression exercés par le dos du conducteur sur le siège avant. Ces données pourraient être réutilisées pour mettre en place un mécanisme de détection de l'assoupissement du conducteur et prévenir ainsi les accidents ; dans le cadre du système actuel, une nouvelle autorisation sera nécessaire car la finalité du traitement est modifiée, alors que les risques pour la vie privée sont négligeables. Le principe de détermination des finalités est aussi accusé d'entraver la combinaison de bases de données constituées dans des buts différents, alors que cette combinaison est souvent créatrice de valeur. Le même ouvrage mentionne une étude réalisée par la Société danoise du cancer relative aux risques de maladie associés à l'utilisation des téléphones mobiles. L'étude s'est basée sur le rapprochement de trois sources constituées pour des finalités tout à fait différentes : les données détenues par les opérateurs de téléphones mobiles, le registre tenu par l'État sur les patients atteints par le cancer et les données fiscales pour connaître le niveau de revenu des personnes. Elle a ainsi pu constituer une base exhaustive d'une grande richesse, dont la réalisation par une enquête *ad hoc* aurait été très coûteuse. Selon le Forum économique mondial, « *à l'ère du* Big Data*, la collecte de données pour des fins déterminées représente une part décroissante de la collecte totale de données* »[279].

Dès lors que la nécessité de déterminer des finalités est en cause, le principe de proportionnalité l'est aussi, puisque la proportionnalité ne peut s'apprécier qu'au regard des finalités[280]. En outre, un des postulats du *Big Data* est que plus le nombre de données collectées est important, plus leur exploitation est susceptible de produire des résultats pertinents. Si un échantillon de taille modeste, bien sélectionné, peut suffire à réaliser des estimations fiables, les possibilités de le segmenter pour observer des corrélations sur des sous-ensembles sont limitées : un échantillon suffisant pour estimer les intentions de vote sur l'ensemble d'un pays ne le sera sans doute pas si l'on souhaite évaluer ces intentions par ville, par quartier ou par immeuble. Une base de données de très grande taille permet de multiplier les requêtes pour détecter des corrélations imprévues ou détecter des « *signaux faibles* » : par exemple, les effets indésirables d'un médicament ne pourront être observés que si le nombre de données traitées dans le cadre de la pharmacovigilance est suffisamment élevé. Compte tenu de la faiblesse des coûts de collecte et de stockage de la donnée, l'idéal du *Big Data* est de tendre à l'exhaustivité, c'est-à-dire au recensement de la totalité de la population que l'on souhaite observer. Entre le *Big Data*, qui tend à la collecte du plus grand nombre de données possibles, et le principe de proportionnalité (parfois dénommé aussi « *principe de minimisation* »), qui vise à limiter la collecte à ce qui est nécessaire, il existe nécessairement une tension.

---

279. World Economic Forum, *Unlocking the Value of Personal Data: From Collection to Usage*, février 2013.

280. Selon l'article 6 de la loi du 6 janvier 1978, les données doivent être « *adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont collectées et de leurs traitements ultérieurs* ».

S'agissant du principe d'exactitude, l'article 6 de la loi du 6 janvier 1978 dispose que les données sont « *exactes, complètes et, si nécessaire, mises à jour* ». Il s'agit d'une obligation de moyens incombant au responsable du traitement, qui doit prendre « *les mesures appropriées (…) pour que les données inexactes ou incomplètes au regard des finalités pour lesquelles elles sont collectées ou traitées soient effacées ou rectifiées* ». Si ce principe a pour objet de protéger la personne concernée, il correspond aussi à l'intérêt du responsable de traitement, que des données inexactes peuvent induire en erreur. Le caractère de plus en plus massif des données traitées pourrait cependant, selon certains, atténuer la nécessité de s'assurer de leur exactitude[281]. Selon Viktor Mayer-Schönberger et Kenneth Cukier, « *l'un des changements les plus fondamentaux qui accompagne aujourd'hui le passage de petits à d'énormes volumes de données* » tient à la possibilité d'en accepter l'imprécision ; l'acceptation de l'imprécision serait même une condition pour obtenir l'augmentation du volume. Dès lors, l'obligation d'exactitude pourrait, de manière paradoxale, nuire à l'exploitation pertinente des données.

Enfin, le principe de limitation de la durée de conservation impose de conserver les données « *sous une forme permettant l'identification des personnes concernées pendant une durée qui n'excède pas la durée nécessaire aux finalités pour lesquelles elles sont collectées et traitées* ». Deux objections sont formulées à l'encontre de ce principe. D'une part, l'effacement des données, lorsque la finalité de leur collecte ne justifie plus leur conservation, empêcherait leur réutilisation ultérieure au service d'autres finalités. D'autre part, certaines personnes souhaitent conserver leurs données sans limitation de durée. Les sites de partage de photographies, les réseaux sociaux ou les messageries électroniques constituent aujourd'hui des réceptacles pour les souvenirs des individus et il est légitime pour ces derniers de s'opposer à un effacement systématique. La question se pose même de la conservation des données après le décès de la personne concernée et des droits qu'ont ses proches sur ces données. La loi du 6 janvier 1978 est aujourd'hui muette à ce sujet, seule la personne concernée ayant des droits sur ses données. Si cette question n'est pour l'instant à l'origine que de peu de litiges, en raison du caractère récent des usages numériques, elle devrait se poser avec une fréquence croissante dans les années à venir. La CNIL a décidé d'inscrire cette question à son programme de travail pour 2014.

• *Le rôle du consentement et du droit d'information*

De manière significative, les interrogations les plus radicales[282] sur le rôle joué par le consentement dans la législation sur les données personnelles émanent aussi bien d'acteurs critiques des développements contemporains du numérique et de leurs

281. Cette affirmation est cependant contestée, l'augmentation de la taille de l'échantillon ne permettant pas de corriger les biais dans la constitution de celui-ci.

282. On ne traite ici que des interrogations remettant en cause le principe même du consentement. Les interrogations sur les modalités de recueil du consentement sont abordées plus loin (cf. *infra* 2.2.3).

risques pour la vie privée, comme l'universitaire américaine Helen Nissenbaum[283], que de milieux d'affaires favorables au développement de l'économie numérique, comme le Forum économique mondial de Davos[284].

Pour Helen Nissenbaum, le recueil du consentement est une fiction, dès lors que les internautes ne peuvent négocier les conditions d'utilisation de leurs données et que la plupart des grands services de la société numérique, qu'il est très difficile de ne pas utiliser, appliquent tous peu ou prou les mêmes procédés ; il n'existe dès lors pas de réelle liberté de choix. La seule liberté qui tend à se développer est celle qui permet aux personnes de choisir entre une version gratuite du site, avec utilisation des données personnelles à des fins publicitaires, et une version payante sans publicité (modèle souvent qualifié de « *freemium* », par contraction des mots anglais « *free* », qui désigne la version gratuite, et « *premium* », pour la version payante de qualité supérieure). Cette liberté induit cependant une inégalité entre internautes selon leurs capacités financières.

Selon le Forum économique mondial, le principe du consentement informé[285] n'est plus adapté à une époque où la plus grande part de la collecte des données se fait de manière automatisée. En outre, le recueil du consentement n'implique la personne que de manière formelle, sans réellement lui donner les moyens de comprendre l'utilisation de ses données ou d'agir sur celle-ci. Le Forum préconise de substituer à cette approche une démarche d'« *empowerment* » de l'individu, développant sa capacité à appréhender l'utilisation de ses données et à la paramétrer par des outils adaptés.

Les principes de la protection des données résistent aux interrogations formulées à leur encontre

Pour nombreuses qu'elles soient, les interrogations relatives aux principes fondamentaux de la protection des données personnelles peuvent et doivent être surmontées. Tant l'approche large de la notion de données personnelles que les principes relatifs à la qualité des données sont indispensables pour assurer la protection des personnes. Le consentement de celles-ci, dont le rôle ne doit certes pas être surestimé, ne peut pour autant être méconnu. Les interrogations les plus fortes, celles qui concernent les usages statistiques du *Big Data*, peuvent en réalité recevoir une réponse dans le cadre juridique actuel.

• *Une définition large des données à caractère personnel est nécessaire pour assurer la protection des personnes*

La question du champ couvert par la notion de donnée personnelle ne présente pas qu'un intérêt purement spéculatif et conceptuel. Cette notion s'inscrit dans

283. H. Nissenbaum, *Privacy in Context: Technology, Policy, and the Integrity of Social Life*,: Stanford University Press, 2010 ; cf. aussi "A Contextual Appproach to Privacy Online", *Daedalus*, vol. 140, no. 4, 2011.

284. World Economic Forum, *Unlocking the Value of Personal Data: From Collection to Usage*, février 2013.

285. « *Notice and consent* », selon la terminologie anglaise.

une législation dont la finalité est de protéger les personnes dont les données sont traitées. C'est au regard de cette finalité que la question de la définition doit être posée. Dès lors qu'une information est susceptible d'être rattachée à une personne, celle-ci doit bénéficier des principes protecteurs de la législation sur les données personnelles ; ceci requiert une définition large.

Les exemples présentés ci-dessus, lors de l'exposé des interrogations, illustrent tous ce besoin de protection.

- L'adresse IP désigne certes, comme l'a jugé la cour d'appel de Paris, une machine et non une personne. Cependant, cette machine peut le plus souvent être rattachée à la personne qui l'a utilisée. Le fournisseur d'accès à internet sait dans la plupart des cas quel est le titulaire de l'abonnement auquel il a attribué telle adresse IP à un instant t. Dans une organisation collective comme une entreprise, une même adresse IP peut être utilisée par un grand nombre de personnes, mais l'administrateur du réseau interne peut reconstituer les connexions opérées par chacun des salariés. Même dans le cas d'un cybercafé, dont les utilisateurs bénéficient d'un certain anonymat, des témoignages peuvent servir à identifier celui qui a utilisé telle machine à telle heure. Dès lors que la machine est rattachée à une personne, l'adresse IP révèle sur celle-ci un nombre considérable d'informations, notamment les sites internet visités et les individus avec lesquels cette personne a correspondu. L'adresse IP doit donc être considérée comme une donnée personnelle.

- Les profils utilisés en matière de publicité en ligne ne comportent peut-être pas l'identité de la personne, mais recèlent un grand nombre d'informations sur une personne donnée. C'est bien cette personne que le publicitaire cherche à toucher, en raison de ses caractéristiques propres. En outre, les données du profil sont susceptibles d'être croisées avec d'autres données concernant la même personne et l'identité de celle-ci peut aisément être retrouvée.

- Une base de données retraçant tous les trajets des utilisateurs du passe Navigo, mais dont les identifiants (l'identité des titulaires d'abonnement) auraient été enlevés et qui ne servirait qu'à mesurer les flux de passagers peut sembler ne pas présenter d'enjeux de protection. Pourtant, les trajets quotidiens de chaque individu sont très caractéristiques, notamment en raison de la récurrence des déplacements du domicile au travail, et ces données peuvent donc être réidentifiées. En outre, la base de données peut être cédée à un tiers qui en fera peut-être d'autres utilisations que la mesure des flux de passagers, présentant plus de risques pour les personnes concernées. Pour que cette cession entre dans le champ de la législation sur les données personnelles, il faut que la base de données elle-même soit qualifiée de traitement de données personnelles.

L'approche large retenue par la CJUE et par les autorités de protection des données réunies au sein du G29 est donc pertinente. Elle n'exclut pas qu'au sein de ce champ large, les obligations des responsables de traitement soient proportionnées au niveau du risque que ce traitement fait courir aux personnes concernées, avec en particulier un faible niveau d'obligations pour les traitements à caractère statistique.

• *Les principes relatifs à la qualité des données sont au cœur de la confiance des personnes dans les services de la société numérique*

Les principes relatifs à la qualité des données se ramènent en réalité à deux familles de principes : le principe de finalités déterminées, avec ses corollaires que sont le principe de proportionnalité et le principe de limitation de la durée de conservation, et le principe général de responsabilité, qui implique de la part du responsable de traitement loyauté et exactitude. Sans respect de ces deux principes fondamentaux, il ne peut y avoir de confiance dans les services de la société numérique.

L'exemple du moteur de recherche permet de le comprendre aisément. Un moteur de recherche collecte et conserve des données à caractère personnel pour deux finalités : fournir le meilleur service possible de recherche sur internet (notamment en personnalisant les résultats en fonction des recherches précédentes) et envoyer des publicités ciblées. La transmission de ces données, riches d'informations sur les personnes concernées, à des organismes de crédit, à des employeurs ou à des enquêteurs privés ou publics porte atteinte aux droits des personnes concernées. Elle ne correspond pas aux finalités du moteur de recherche, et méconnaît ainsi la confiance que l'utilisateur a pu placer dans ce service. Une telle transmission ne pourrait être envisagée que si elle était autorisée par la loi, pour une finalité d'intérêt public, par exemple pour les besoins d'une enquête judiciaire.

Le **principe de finalités déterminées** est ainsi au cœur de la confiance que les personnes peuvent avoir dans les services de la société numérique. Lorsqu'elles recourent à de tels services et que des données les concernant sont collectées dans ce cadre, elles doivent avoir l'assurance que ces données ne seront pas utilisées pour d'autres finalités que celles du service, sauf à ce qu'elles en aient été informées ou que la loi le prévoie. Le principe de finalités déterminées est ce qui fait que les données personnelles ne sont pas des marchandises ou, du moins, qu'elles ne sont pas des marchandises comme les autres : elles peuvent être échangées, mais le droit de propriété de leur acquéreur reste limité par les droits de la personne sur ses données, qui impliquent que leur utilisation soit limitée aux finalités pour lesquelles elles ont été initialement collectées (cf. *infra* 3.1.3 pour de plus amples développements sur le droit de propriété et les données personnelles). En outre, ce n'est que si les finalités sont déterminées qu'il est possible de s'assurer de leur **légitimité**, autre exigence formulée par l'article 6 de la loi du 6 janvier 1978[286].

Les principes de **proportionnalité** et de **limitation de la durée de conservation** découlent de ce premier principe. Si les données ne doivent être traitées que pour des finalités déterminées, il n'est pas légitime de collecter des données qui ne seraient pas utiles à ces finalités ou de les conserver plus longtemps que ce qui est justifié par ces dernières. Le souhait d'une personne de voir conservées

286. Pour un exemple de traitement de données refusé par la CNIL en raison du caractère illicite de sa finalité, cf. la délibération n° 2007-191 du 10 juillet 2007 : la CNIL estime que le traitement envisagé par la société Infobail, consistant en un fichier recensant les impayés de loyers des locataires d'immeubles d'habitation était susceptible de porter atteinte au droit au logement.

ses données sans limitation de durée est légitime ; aussi l'article 36 de la loi du 6 janvier 1978 permet-il déjà de déroger au principe de limitation avec l'accord exprès de la personne concernée.

Quant aux principes de **loyauté de la collecte** et **d'exactitude** des données traitées, ils ne sont que l'expression des principes généraux de la responsabilité : collecter des données de manière déloyale, c'est surprendre la confiance de la personne concernée et commettre ainsi une faute à son égard ; il est raisonnable d'attendre de celui qui traite des données personnelles, dans l'optique de produire des conséquences pour les personnes concernées, qu'il s'assure de la véracité des informations qu'il utilise. Si ces deux principes n'avaient pas été prévus par la loi, le juge les aurait déduits des principes généraux de la responsabilité.

• *Le rôle du consentement ne doit pas être surestimé mais ne peut être méconnu*

Le rôle joué par le consentement de la personne dans la législation actuelle ne doit pas être surestimé. Le consentement n'est pas une condition nécessaire pour que des données soient traitées légalement : l'article 7 de la loi du 6 janvier 1978 permet de traiter des données sur la base d'autres fondements, tels que l'existence d'une obligation légale ou l'intérêt légitime du responsable de traitement. Il n'est pas non plus une condition suffisante : il ne dispense pas le responsable de traitement de respecter les principes énoncés par l'article 6.

Pour autant, le principe énoncé par l'article 8 de la Charte des droits fondamentaux de l'Union européenne, selon lequel les données ne peuvent être traitées qu'avec le consentement de la personne, sauf autre fondement légitime prévu par la loi, touche au sens même de la protection des données et doit être maintenu. Des débats existent sur le moment et les modalités de recueil du consentement, mais ils se situent au niveau des instruments de la protection. Dans son principe, l'obligation de recueil du consentement tend à reconnaître la liberté de la personne en matière d'utilisation de ses données personnelles[287]. Des approches qui nieraient cette liberté en postulant la liberté de réutilisation des données personnelles indépendamment de la volonté de la personne concernée ou qui affirmeraient à l'excès la nécessité d'une intervention tutélaire de la puissance publique, définissant ce qu'un individu considéré comme incapable de veiller à ses données a le droit d'en faire, ne peuvent être suivies.

• *Les interrogations soulevées par les usages du* Big Data *à caractère statistique peuvent recevoir une réponse dans le cadre juridique actuel*

L'expression générique de *Big Data* recouvre trois catégories d'usages différents :

- Des usages qui ne portent pas sur des données à caractère personnel, par exemple l'optimisation de la maintenance des véhicules par l'utilisation des données transmises par des capteurs ou la construction d'indices de prix par la collecte des prix des biens et services commercialisés sur internet.

287. Liberté qui sera plus loin analysée au regard du concept allemand « *d'autodétermination informationnelle* » (cf. *infra* 3.1.1).

- Des usages qui portent sur des données à caractère personnel mais qui ont une finalité statistique : c'est le cas de l'application *Google Flu Trends*, qui détecte les épidémies de grippe à partir des requêtes formulées par les internautes sur le moteur de recherche, ou de l'utilisation des bases de données de l'assurance-maladie pour détecter les effets indésirables d'un médicament. Dans ce type d'usage, les données personnelles sont souvent désidentifiées.

- Des usages non statistiques qui portent sur des données à caractère personnel : c'est le cas de la publicité comportementale, du repérage des fraudes par des organismes de sécurité sociale identifiant des profils-types de fraudeurs ou de l'évaluation du risque de défaut d'un emprunteur.

La première catégorie échappe totalement au cadre juridique de la protection des données à caractère personnel. La troisième catégorie appelle la pleine application des principes relatifs à la qualité des données présentés ci-dessus. En revanche, la catégorie intermédiaire, celle des usages à finalité statistique, bénéficie déjà, dans le cadre juridique actuel, de dispositions de nature à répondre aux interrogations exposées ci-dessus. En effet, plusieurs assouplissements sont prévus pour les usages statistiques ou les traitements de données appelées à être anonymisées :

- L'article 6 de la loi du 6 janvier 1978 dispose qu'un traitement ultérieur des données à des fins statistiques est considéré comme compatible avec les finalités initiales du traitement, à condition notamment de respecter les procédures prévues par le chapitre IV de la loi (déclaration du traitement statistique à la CNIL) et les obligations prévues par le chapitre V (obligation d'information des personnes concernées et d'assurer la sécurité des données), et de ne pas être utilisé pour prendre des décisions à l'égard des personnes concernées.

- L'article 8 permet de déroger à l'interdiction de collecter et de traiter des données sensibles, pour les seuls traitements réalisés par les services de la statistique publique (INSEE et services statistiques ministériels) dans le cadre de la loi du 7 juin 1951 sur l'obligation, la coordination et le secret en matière de statistiques, après autorisation de la CNIL.

- De manière générale, le traitement de données sensibles peut être autorisé par la CNIL si ces données sont appelées à faire l'objet à bref délai d'un procédé d'anonymisation reconnu conforme par elle.

- L'obligation d'information prévue par l'article 32 est allégée lorsque les données sont appelées à faire l'objet à bref délai d'un procédé d'anonymisation reconnu conforme par la CNIL.

- Il peut être dérogé au principe de limitation de la durée de conservation pour les traitements réalisés à des fins historiques, statistiques ou scientifiques.

- Enfin, s'agissant des informations publiques[288], l'article 10 de la loi du 17 juillet 1978 dispose qu'elles « *peuvent être utilisées par toute personne qui le souhaite*

288. Définies par l'article 1er de la loi du 17 juillet 1978 comme l'ensemble des documents produits ou reçus, dans le cadre de leur mission de service public, par l'État, les collectivités territoriales ainsi que par les autres personnes de droit public ou les personnes de droit privé chargées d'une mission de service public.

à d'autres fins que la mission de service public pour les besoins de laquelle les documents ont été produits ou reçus ». Lorsque ces informations publiques comportent des données à caractère personnel, l'article 13 de la même loi autorise leur réutilisation à d'autres fins à condition que les personnes concernées aient donné leur consentement, que la personne détentrice soit en mesure de les anonymiser ou qu'une disposition législative l'autorise.

On constate donc que le droit actuel consacre déjà la liberté de réutiliser les données à caractère personnel à d'autres fins que celles qui ont justifié leur collecte, dès lors que ces fins ont un caractère statistique. Tous les usages du *Big Data* dont l'objet est d'établir des corrélations entre les ensembles de données et non de s'intéresser aux personnes de manière individuelle peuvent bénéficier de ces dispositions, leur finalité pouvant être qualifiée de statistique. De même, pour ces usages à finalité statistique, aucune limitation de la durée de conservation n'est imposée. Enfin, d'autres assouplissements sont possibles, concernant le traitement des données sensibles, l'information des personnes concernées et la réutilisation des données publiques, si les données font l'objet d'un procédé d'anonymisation.

Les principes actuels ne sont donc pas par eux-mêmes un obstacle à la réutilisation des données personnelles à des fins statistiques, qui est essentielle pour le développement du *Big Data*. Le cas échéant, le recours à des méthodes de « *pseudonymisation* »[289], consistant à séparer les données directement identifiantes des données traitées, peut contribuer à renforcer l'assurance que les données ne sont traitées qu'à des fins statistiques.

2.1.3. Les instruments de la protection des données doivent en revanche être transformés

Les limites des instruments de mise en œuvre de la protection

Les interrogations relatives aux instruments portent sur les modalités d'information et de recueil du consentement des personnes concernées par les traitements de données, le mode d'intervention des autorités de protection et le champ d'application territorial de la protection.

---

289. Les données pseudonymes sont définies par la version de la proposition de règlement de l'Union européenne sur la protection des données personnelles votée par le Parlement européen le 12 mars 2014 comme « *des données à caractère personnel qui ne peuvent pas être attribuées à une personne concernée sans avoir recours à des informations supplémentaires, pour autant que de telles informations supplémentaires soient conservées séparément et soumises à des mesures techniques et organisationnelles afin de garantir cette non-attribution* ». La pseudonymisation se distingue de l'anonymisation en ce qu'elle ne supprime pas toute possibilité d'identification, mais la rend seulement plus difficile. Elle peut passer notamment par la transmission des données d'identification à un « tiers de confiance » distinct de l'organisme traitant les données, qui serait seul capable de faire le lien entre les personnes et les données les concernant.

• *Les modalités d'information et de recueil du consentement*

Il est communément admis aujourd'hui que pour la grande majorité des services proposés sur les réseaux numériques, les modalités de recueil du consentement et d'information ne sont pas satisfaisantes. Les conditions générales d'utilisation (CGU) et les *policies* des sites internet relatives à la protection des données personnelles sont souvent très longues, écrites en termes techniques et difficiles d'accès ; elles sont en outre fréquemment modifiées. Il suffit souvent de cocher une simple case pour être réputé les avoir lues ; pour certains sites, la consultation ne constitue même pas un préalable pour l'accès au service, l'internaute ayant seulement la possibilité de cliquer sur le lien vers cette information. Plusieurs des personnes auditionnées dans le cadre de cette étude, pourtant particulièrement conscientes des enjeux de protection de la vie privée, ont confessé ne jamais prendre le temps de consulter ces documents. La démarche peut être perçue par l'internaute comme ayant d'autant moins d'intérêt qu'il s'agit de contrats d'adhésion, dont le contenu ne peut être négocié. Dès lors, on peut s'interroger sur le respect effectif des conditions prévues par la directive n° 95/46/CE pour qu'il y ait consentement : selon l'article 2, le consentement est une « *manifestation de volonté, libre, spécifique et informée par laquelle la personne concernée accepte que des données à caractère personnel la concernant fassent l'objet d'un traitement* ».

De même, la règle prévue par l'article 32 de la loi du 6 janvier 1978, selon laquelle la personne doit être informée même lorsque les données ne sont pas recueillies auprès d'elle n'est manifestement pas appliquée de manière systématique. Les transactions portant sur les données personnelles ne donnent pas lieu en règle générale à des notifications, pas plus que les opérations tendant à collecter les informations disponibles en ligne sur une personne ; les acteurs concernés semblent toujours considérer qu'une telle information exigerait « *des efforts disproportionnés par rapport à l'intérêt de la démarche* ». Dans son arrêt précité du 12 mars 2014, le Conseil d'État a pourtant confirmé la position de la CNIL selon laquelle la société Pages Jaunes, lorsqu'elle procédait à la collecte d'informations sur les réseaux sociaux pour les agréger à son service Pages Blanches, était tenue à une obligation d'information en vertu de l'article 32 de la loi du 6 janvier 1978 ; il a jugé « *qu'eu égard à l'intérêt qui s'attache au respect des libertés et droits fondamentaux des vingt-cinq millions de personnes touchées par le traitement litigieux, et notamment au respect de leur vie privée, la société Pages Jaunes Groupe n'est pas fondée à soutenir que l'information de ces personnes, dont elle avait les coordonnées, exigeait des efforts disproportionnés par rapport à l'intérêt de la démarche* ».

• *Le mode d'intervention des autorités de protection*

Le mode d'intervention de la CNIL, comme de ses homologues européens, repose notamment sur l'obligation de déclaration des traitements de données. Les articles 22 et 23 de la loi du 6 janvier 1978 imposent une déclaration préalable avant la mise en œuvre de tout traitement. La déclaration doit indiquer l'identité du responsable du traitement, les finalités de celui-ci, les données traitées et les catégories de destinataires ; une nouvelle information de la CNIL doit être effectuée lors de toute modification de l'un de ces éléments. La méconnaissance de l'obligation

de déclaration expose le responsable de traitement à de lourdes conséquences, tant sur le plan pénal (cinq ans d'emprisonnement et 300 000 euros d'amende[290]) que commercial (nullité de la vente d'un fichier non déclaré à la CNIL[291]) ou, pour les traitements de données concernant les salariés, sur le plan du droit du travail (absence de cause réelle et sérieuse d'un licenciement justifié par des données collectées dans le cadre d'un traitement non déclaré[292]).

Ce système s'expose à différents reproches. Il conduit à transmettre à la CNIL une masse considérable d'informations, d'inégal intérêt en raison des enjeux très variables pour la protection des données personnelles[293]. Si l'obligation de déclaration est assez simple à respecter pour des entreprises ne mettant en œuvre que des traitements courants (par exemple, un fichier du personnel et un fichier des clients), elle peut s'avérer plus lourde pour des acteurs, notamment ceux de l'économie numérique, qui ont une activité intense et évolutive de traitement des données. Les « *startups* », en particulier, sont susceptibles de voir évoluer au cours de leurs premières années leur modèle d'affaires et, corrélativement, leurs modalités d'utilisation des données personnelles ; en raison de leur petite taille, elles peuvent avoir plus de difficulté à appréhender leurs obligations de déclaration et sont ainsi exposées à une certaine insécurité juridique. Pour autant, l'obligation de déclaration ne met pas à disposition de la CNIL toutes les informations nécessaires pour évaluer le degré de sensibilité d'un traitement ; en particulier, la CNIL n'est informée ni du nombre de personnes dont les données sont traitées, ni du volume des données transmises à des tiers.

L'article 22 de la loi du 6 janvier 1978 permet aux responsables de traitement d'opter pour un autre système en désignant un « *correspondant à la protection des données à caractère personnel* », couramment dénommé « *correspondant informatique et libertés* » (CIL), qui est chargé « *d'assurer, d'une manière indépendante, le respect des obligations* » prévues par la loi ; ils sont alors dispensés des obligations de déclaration. Le principal avantage de la désignation d'un CIL est qu'elle tend à assurer le respect de la loi de manière continue et pas seulement au

290. Article 226-16 du code pénal.

291. Com. 25 juin 2013, n° 12-17.037. L'arrêt vise l'article 1128 du code civil, selon lequel « *il n'y a que les choses qui sont dans le commerce qui puissent être l'objet des conventions* » ; la Cour de cassation a jugé qu'un fichier non déclaré à la CNIL n'était pas dans le commerce.

292. Soc., 6 avril 2004, n° 01-45.227.

293. En 2013, la CNIL a reçu 35 931 « *déclarations normales* » et 50 832 « *déclarations simplifiées* ». Des déclarations simplifiées peuvent être effectuées notamment sur le fondement de l'article 24 de la loi, pour « *les catégories les plus courantes de traitements de données à caractère personnel, dont la mise en œuvre n'est pas susceptible de porter atteinte à la vie privée ou aux libertés* » ; la CNIL publie alors des normes et les responsables de traitement doivent seulement déclarer leur conformité à ces normes. Les normes adoptées par la CNIL sur ce fondement concernent notamment les données gérées par certaines professions dans le cadre de leur activité ou d'autres types d'opérations courantes : pharmaciens, assureurs, fichiers de gestion de clients, de gestion du personnel, etc.

stade de l'obligation formelle de déclaration. Cependant, seule une minorité de responsables de traitement ont procédé à la désignation d'un CIL, même si leur nombre est en croissance rapide[294].

Les pouvoirs de sanction et de contrôle souffrent de certaines limites. Les sanctions que peut prononcer la CNIL sont limitées à 150 000 euros ou 300 000 euros en cas de réitération. De tels montants ne présentent pas de caractère dissuasif pour des acteurs économiques de taille importante ou même seulement moyenne[295]. S'agissant des contrôles, il a fallu attendre la loi du 17 mars 2014 relative à la consommation pour que la CNIL dispose, en plus de ses prérogatives de contrôle sur place et sur pièces et de ses pouvoirs de convocation, d'une capacité légale à procéder à des constatations sur les données librement accessibles en ligne.

• *Le caractère national de la protection*

Si elle harmonise les législations de chaque État, la directive n° 95/46/CE maintient le caractère national de l'organisation de la protection. Selon son article 4.1. a), la législation de chaque État est applicable lorsque le traitement est effectué « *dans le cadre des activités d'un établissement du responsable de traitement sur le territoire de l'État membre* ». Lorsque le responsable de traitement est établi dans plusieurs États, il doit respecter le droit de chacun d'entre eux. L'article 28 dispose que chaque autorité de contrôle nationale est compétente pour exercer ses pouvoirs d'investigation sur son territoire.

La territorialité de la protection des données personnelles présente plusieurs difficultés, toutes liées à son inadéquation au caractère souvent transnational des traitements de données. Le fait pour les responsables de traitement de devoir se conformer aux droits de différents États membres est un facteur de complexité important et peut être un obstacle au développement des entreprises. Lorsqu'un même traitement est opéré dans plusieurs États, chaque autorité nationale dispose d'une vision partielle et le système est susceptible d'aboutir à des décisions discordantes. La coordination des autorités au sein du G29 peut pallier cette difficulté, comme le montre la procédure entreprise à l'encontre de *Google*, mais elle conduit de manière inévitable à alourdir le processus de décision, alors que la célérité de l'action est essentielle face à des usages numériques qui évoluent rapidement. Enfin, la mise en œuvre de ces règles de territorialité fait l'objet de controverses. Dans un arrêt *Google Spain* du 13 mai 2014, la CJUE a retenu une interprétation large de l'article 4.1 a) : la filiale *Google Spain*, établie en Espagne, n'exerce pas de responsabilités dans le fonctionnement technique du moteur de recherche de la société *Google* ; la CJUE a cependant considéré que le traitement de données devait être regardé comme effectué dans le cadre des activités de *Google Spain*, en raison du caractère indissociable du moteur de recherche et des

294. En 2013, près de 13 000 organismes publics ou privés avaient désigné un correspondant, contre 8 500 en 2011.

295. De manière significative, la société *Google*, qui a fait l'objet d'une sanction de 150 000 euros prononcée par une délibération de la CNIL du 3 janvier 2014, n'a demandé en référé que la suspension de l'injonction de publier sur son site un communiqué relatif à cette sanction, et non celle de la sanction elle-même.

opérations de promotion et de vente des espaces publicitaires qui en assurent le financement et dont est chargée cette filiale (CJUE, Gde Ch., 13 mai 2014, *Google Spain c/ AEPD*, C-131/12, 4° du dispositif). Quant à l'article 4.1 c) de la directive, il dispose que le droit d'un État membre est applicable à un responsable de traitement établi en dehors de l'Union européenne si celui-ci « *recourt, à des fins de traitement de données à caractère personnel, à des moyens, automatisés ou non, situés sur le territoire dudit État membre* ». La position du G29 est que l'installation de *cookies* sur le terminal d'un internaute résidant dans l'Union européenne constitue un tel « *moyen* » situé sur le territoire d'un État membre[296], mais cette interprétation fait l'objet de contestations. La question est actuellement pendante dans le cadre d'une instance devant le Conseil d'État[297]. Compte tenu de l'audience des services fournis par des sociétés établies en dehors de l'Union européenne, elle présente un caractère déterminant.

Les instruments de la protection des données doivent être profondément transformés

Quatre voies complémentaires devraient être explorées pour rénover les instruments de la protection des données : l'utilisation des technologies pour renforcer la capacité des personnes à contrôler l'utilisation de leurs données ; la définition d'une « chaîne de responsabilités », allant des concepteurs de logiciels et d'objets connectés aux utilisateurs finaux et complétant la responsabilité du responsable de traitement ; une attention particulière portée à la circulation des données personnelles ; le passage d'une logique formelle de déclaration à une logique de respect en continu de la réglementation, assuré par des contrôles internes et externes. Les moyens de les mettre en œuvre seront développés dans les propositions de la troisième partie.

• *L'utilisation des technologies pour renforcer la capacité des personnes à contrôler l'utilisation de leurs données*

Les technologies numériques conduisent à une dissémination croissante des données personnelles. Cependant, elles peuvent aussi être utilisées pour protéger la vie privée des individus. Au sein de la famille des « *Privacy Enhancing Technologies* » (technologies renforçant la protection de la vie privée), deux catégories peuvent être distinguées : celles qui visent à rendre les données moins accessibles aux tiers (a) et celles qui visent à renforcer la maîtrise de la personne sur l'utilisation de ses données par les tiers (b).

(a) La première catégorie couvre l'ensemble des moyens de cryptologie, les « réseaux privés virtuels » qui permettent à leurs utilisateurs de modifier leurs adresses IP ou encore le réseau TOR, qui permet de rendre anonymes les échanges sur internet. L'utilisation de ces procédés, qui peuvent rendre des services appréciables aux personnes soucieuses de la confidentialité de leurs communications, est légale ; la LCEN a, en particulier, disposé que « *l'utilisation des moyens de cryptologie est*

296. Article 29 Data Protection Working Party, "Opinion 8/2010 on applicable law", décembre 2010, WP 179.

297. Affaire n° 374594, *Google Inc c/ CNIL*.

libre ». Toutefois, ces procédés sont aussi employés pour protéger des activités illicites et leur diffusion peut rendre plus difficile l'action des services de police. Il n'y a donc pas lieu pour les pouvoirs publics d'encourager cette diffusion.

(b) En revanche, les technologies appartenant à la seconde catégorie ne soulèvent pas les mêmes difficultés : elles sont de nature à renforcer la protection de la vie privée sans présenter de risques pour l'ordre public. Les procédés permettant de renforcer la maîtrise de la personne sur l'utilisation de ses données sont variés :

- Les principaux navigateurs disponibles sur le marché offrent la possibilité à leurs utilisateurs de bloquer l'enregistrement de *cookies* sur leur terminal.

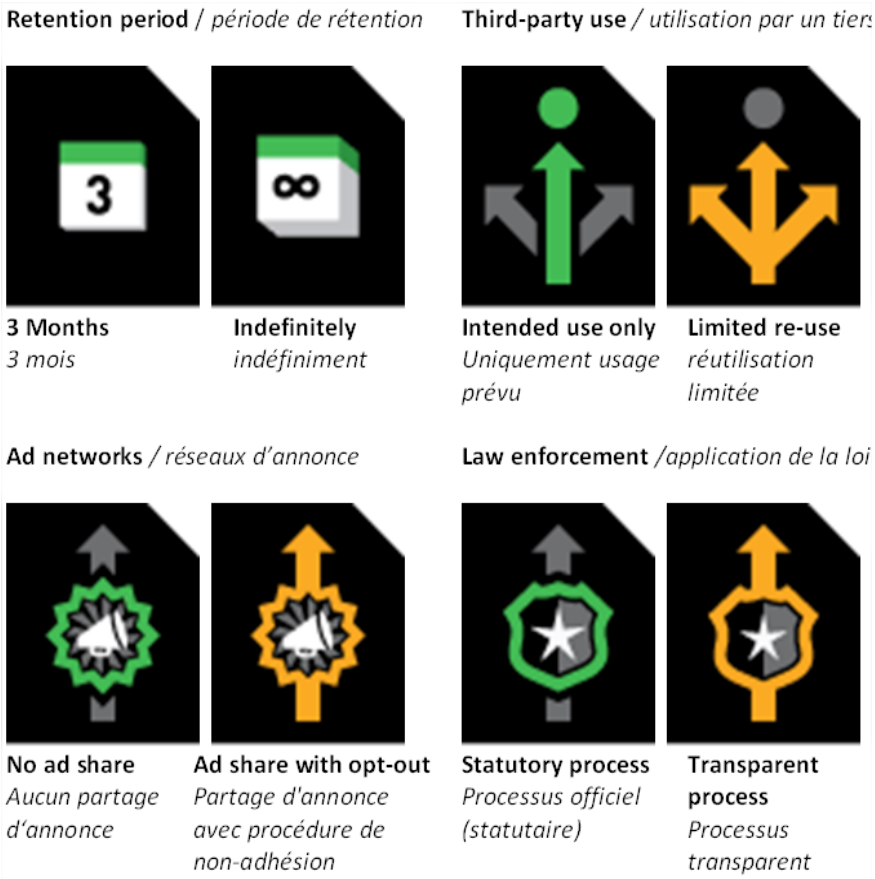
- Un standard dénommé « *Do Not Track* » est en cours d'élaboration au sein du *World Wide Web Consortium* (W3C) : il permettrait aux internautes d'exprimer leurs préférences en matière de traçage de leurs données par les *cookies* ou d'autres outils, dans un langage universellement reconnu par tous les sites visités.

- Le projet « Mes Infos » de la Fondation internet nouvelle génération (FING), consiste à donner aux individus une plateforme d'accès à l'ensemble des données personnelles détenues par un ensemble de partenaires[298]. Les données personnelles disséminées sont donc rassemblées dans une plateforme, dont seul l'individu maîtrise l'accès. Un projet similaire dénommé My Data est conduit par le gouvernement britannique. Au-delà de ces projets, des solutions de gestion des données personnelles destinées aux particuliers sont également proposées par des acteurs privés.

- Dans son ouvrage *Code is Law*, Lawrence Lessig envisageait la mise en place d'une standardisation généralisée des politiques d'utilisation des données personnelles mises en place par chaque site[299]. Cette standardisation permettrait à chaque site d'indiquer sa politique (par exemple, s'il cède les données collectées à des tiers ou la durée pendant laquelle il les conserve) dans un format simple et lisible par ordinateur en raison de sa standardisation. Du point de vue des internautes, le protocole leur permettrait de définir les paramètres d'utilisation de leurs données qu'ils acceptent ; une incompatibilité entre les préférences de l'internaute et la politique du site serait automatiquement signalée. Si la standardisation généralisée envisagée par Lawrence Lessig n'a pas eu lieu, des démarches permettant aux utilisateurs d'appréhender de manière simple la politique d'utilisation des données personnelles d'un site ont été développées, par exemple le site de notation www.privacyscore.com ou la signalétique préconisée par la *Fondation Mozilla*.

298. Parmi lesquels *Google*, *Orange*, *Axa*, *La Banque Postale* et *Les Mousquetaires*.
299. Qu'il dénomme "*Platform for Privacy Preferences*" ou "*P3P*".

Signalétique d'information sur l'utilisation des données personnelles développée par la fondation Mozilla



Source : Mozikka Wiki, Privacy Icons project (beta release), Owner: Ben Moskowitz, Mozilla; Aza Raskin (initiator), Designs by Michael Nieling & Ocupop, designers of the official HTML5 logos, Updated : June 15, 2011, https://wiki.mozilla.org/Privacy_Icons

- Les données personnelles échangées pourraient être accompagnées de métadonnées, qui indiqueraient par exemple les finalités pour lesquelles les données ont été initialement collectées. Ces métadonnées indiqueraient ainsi à l'ensemble des organismes accédant aux données les limites de leurs droits d'utilisation.

- Enfin, l'intervention de prestataires « *tiers de confiance* », jouant un rôle d'intermédiation dans la relation entre la personne et les organismes traitant ses données personnelles, pourrait être développée. Elle permettrait de garantir que ces organismes n'ont accès qu'aux données dont la personne a autorisé la divulgation, ce qui peut notamment exclure les données d'identification[300].

300. La Fondation Internet Nouvelle Génération (FING) qualifie cette fonction de « *tiers d'anonymisation* » : cf. FING, *Nouvelles approches de la confiance numérique*, février 2011, http://doc.openfing.org/CONFIANCE/ConfianceNumerique_SyntheseFinale_Fevrier2011.pdf

Ces outils technologiques, dont l'étude du Conseil d'État de 1998 sur *Internet et les réseaux numériques* avait déjà relevé le potentiel, sont encore peu utilisés, faute d'appropriation par le grand public ou d'incitation des acteurs du numérique à les mettre en place. Le droit les a encore peu pris en compte, même si des initiatives intéressantes ont été conduites par des acteurs publics, comme l'outil *CookieViz* mis à disposition des internautes par la CNIL, qui permet de visualiser en temps réel l'installation des *cookies* au fil de la navigation sur internet. Le développement de ces outils et de leur utilisation par les individus est un des leviers d'une protection rénovée des données personnelles.

• *La définition d'une chaîne de responsabilité dans la protection des données personnelles*

La législation actuelle ne reconnaît qu'un seul responsable en matière de protection des données personnelles, qu'elle qualifie de « *responsable de traitement* » et qu'elle définit comme la personne qui détermine les finalités et les moyens du traitement. Si elle appréhende l'existence de sous-traitants, elle les considère comme des mandataires transparents du responsable de traitement, agissant « *pour son compte* » et ne déchargeant celui-ci d'aucune de ses responsabilités.

Bien d'autres acteurs interviennent pourtant dans le traitement des données personnelles et jouent ainsi un rôle dans la mise en oeuvre de leur protection :

- Le responsable de traitement utilise souvent des logiciels qui ne sont pas conçus par lui mais dont le fonctionnement contribue de manière positive ou négative à la protection ; les **éditeurs de logiciels** ont donc une part de responsabilité.

- Le développement des objets connectés conduit nécessairement à un rôle croissant des **fabricants** de ces objets. Il est déjà manifeste aujourd'hui que la conception des terminaux tels que les smartphones joue un rôle important dans la protection des données personnelles de leurs utilisateurs et des tiers.

- Le rôle des **sous-traitants** s'est développé de manière considérable avec l'essor de l'informatique en nuage. Les prestataires d'informatique en nuage ont souvent un poids économique supérieur à celui du responsable de traitement et lui imposent des conditions générales d'utilisation, au point que le critère de « *détermination des moyens* » du traitement retenu par la loi pour désigner le responsable peut parfois être délicat à apprécier.

- Enfin, les **particuliers** jouent un rôle sans cesse croissant dans la collecte et le traitement des données personnelles. Ils livrent un grand nombre d'informations concernant les tiers sur les réseaux sociaux. Avec le développement des drones civils, la miniaturisation des dispositifs de captation d'images et de sons ou les progrès de la reconnaissance faciale, ils pourraient devenir des collecteurs de données personnelles de plus en plus puissants. La responsabilité des particuliers n'est aujourd'hui appréhendée que par le droit pénal, dont les sanctions sont rarement appliquées.

La place centrale du responsable de traitement dans la protection des données doit être maintenue, afin d'éviter une dilution des responsabilités. Cependant, les obligations du responsable de traitement devraient être complétées par la définition d'une « chaîne de responsabilités », allant des éditeurs de logiciels et des fabricants d'objets connectés en amont aux particuliers en aval. Les éditeurs de logiciels et les fabricants doivent intégrer dans leur activité le souci de la protection des données, ce à quoi tend le principe de « protection des données dès la conception » (en anglais « *privacy by design* »). Les sous-traitants doivent s'assurer que les moyens fournis au responsable du traitement le mettent en mesure de s'acquitter de ses obligations. Les particuliers doivent mesurer les implications du principe général de responsabilité : en matière de données personnelles comme en tout autre domaine, la liberté consiste à faire tout ce qui ne nuit pas à autrui.

La corégulation peut contribuer à la responsabilisation des acteurs professionnels. L'exemple américain montre les limites de l'autorégulation. En revanche, en complément de la réglementation publique et du rôle exercé par les autorités de protection, des codes de bonne conduite élaborés par les principaux acteurs professionnels concernés pourraient aider à la diffusion et à l'appropriation des bonnes pratiques dans les entreprises adhérentes. Conformément aux préconisations de l'étude annuelle de 2013 du Conseil d'État sur *Le droit souple*, plusieurs conditions doivent être réunies pour que de tels codes de conduite soient légitimes et effectifs : ils doivent être élaborés de manière transparente, en associant l'ensemble des parties prenantes, notamment les consommateurs, leurs associations, les organisations de défense des droits de l'homme et les autorités de protection des données ; ils doivent prévoir des mécanismes d'évaluation de leur mise en œuvre. Il pourrait être envisagé que l'autorité de protection des données homologue les codes de conduite professionnels lorsqu'ils sont conformes à ces conditions.

• *Une plus grande attention à la circulation des données personnelles*

La transmission de données personnelles[301] d'une entité à une autre est porteuse de risques particuliers : dès lors que l'acquéreur des données est une autre entité que celle qui les a initialement collectées auprès de la personne concernée, ses finalités peuvent être différentes. En outre, en dépit des dispositions de l'article 32 de la loi du 6 janvier 1978 sur le droit d'information, la personne concernée n'est que rarement informée de la cession de ses données et ne sait donc plus qui est le responsable de leur traitement. Le risque s'accroît lorsque les transmissions se succèdent. L'arrêt de la chambre commerciale de la Cour de cassation du 25 juin 2013, sanctionnant de nullité la vente d'un fichier non déclaré à la CNIL, est de nature à inciter les acquéreurs à la vigilance sur la régularité des données qu'ils achètent. Toutefois, si l'obligation de déclaration devait être remise en cause, comme l'envisage la proposition de règlement européen (cf. *infra*), la portée de cet arrêt le serait également.

301. Qui peut se faire par la cession de base de données ou l'ouverture d'un droit d'accès pour le tiers à ces données. Les grandes plateformes (cf. *infra* 2.3) ouvrent souvent à des tiers l'accès à leurs données *via* des interfaces de programmation d'applications (API).

• *D'une logique formelle de déclaration à une logique de respect en continu de la réglementation*

Face à la massification des données, les autorités de protection ont besoin de relais, tant internes qu'externes aux responsables de traitement. En interne, le délégué à la protection des données, ou « correspondant informatique et libertés », créé par la directive n° 95/46/CE, peut jouer ce rôle : il dispose de garanties d'indépendance à l'égard du responsable de traitement et a pour mission de s'assurer de manière continue du respect de la réglementation. Sa désignation, aujourd'hui facultative, pourrait devenir obligatoire au-delà d'une certaine taille du responsable de traitement ou d'un certain degré de sensibilité du traitement. En externe, des procédures de certification, tendant à faire attester par un tiers accrédité par l'autorité de protection que le responsable du traitement s'est conformé à la réglementation, pourraient être développées, voire rendues obligatoires pour certaines catégories de traitement. L'objectif est que les responsables de traitement développent une démarche de conformité, en s'assurant du respect de la réglementation dans l'ensemble de leurs processus de travail.

2.1.4. L'arrêt *Google Spain* de la CJUE et la proposition de règlement européen relatif à la protection des données personnelles s'engagent à juste titre dans la voie de la réaffirmation des principes et de la rénovation des instruments

L'arrêt Google Spain c/ AEPD *renforce la maîtrise des individus sur leurs données personnelles en ligne mais suscite des interrogations sur la conciliation entre droit à la vie privée et liberté d'expression*

• *Un arrêt qui consacre le « droit à l'oubli » par le droit au déréférencement*

Outre la question du champ d'application territorial des législations nationales relatives à la protection des données personnelles, examinée plus haut (cf. *supra* 2.3.1), l'arrêt *Google Spain c/ AEPD* est d'une importance majeure à deux égards : il définit pour la première fois les responsabilités en matière de protection des données personnelles d'une catégorie d'acteurs numériques, les moteurs de recherche ; il ouvre la voie à un véritable « droit à l'oubli » des particuliers, reposant sur le droit au déréférencement.

L'affaire ayant donné lieu à cet arrêt concerne un particulier espagnol qui a fait l'objet en 1998 d'une saisie et d'une vente aux enchères d'un de ses biens immobiliers, dans le cadre d'une procédure de recouvrement de dettes de sécurité sociale. Des annonces concernant cette vente aux enchères ont alors été publiées par un journal quotidien. En 2010, ce particulier a saisi l'autorité de protection des données espagnole (AEPD) d'une réclamation pour obtenir le retrait de cette information du site du quotidien et son déréférencement du moteur de recherche *Google*, car cette information s'affichait toujours lorsqu'il saisissait son nom sur ce moteur. L'AEPD a rejeté la demande dirigée contre le quotidien, au

motif que la publication était légalement justifiée, mais a fait droit à sa demande de déréférencement. *Google* a contesté cette décision devant une juridiction espagnole, qui a saisi la CJUE d'un renvoi préjudiciel.

La CJUE s'est d'abord prononcée sur la qualification du moteur de recherche en tant que responsable d'un traitement de données à caractère personnel. *Google* contestait cette qualification, au motif que son algorithme traitait les pages des sites référencés sans égard au caractère personnel ou non des données qu'elles contenaient. L'avocat général de la CJUE avait conclu en ce sens, mais la Cour ne l'a pas suivi. Elle s'est d'abord fondée sur la lettre de la directive n° 95/46/CE, en jugeant qu'« *en explorant de manière automatisée, constante et systématique internet à la recherche des informations qui y sont publiées, l'exploitant d'un moteur de recherche «collecte» de telles données qu'il «extrait», «enregistre» et «organise» par la suite dans le cadre de ses programmes d'indexation, «conserve» sur ses serveurs et, le cas échéant, «communique à» et «met à disposition de» ses utilisateurs sous forme de listes des résultats de leurs recherches* » et que « *ces opérations étant visées de manière explicite et inconditionnelle à l'article 2, sous b), de la directive 95/46, elles doivent être qualifiées de «traitement» au sens de cette disposition* » (§ 28) ; l'exploitant d'un moteur de recherche déterminant « *les finalités et les moyens* » de ces opérations, il est le responsable d'un traitement de données personnelles (§ 32). Elle s'est également appuyée sur un raisonnement téléologique : elle a relevé que « *l'activité d'un moteur de recherche est (…) susceptible d'affecter significativement et de manière additionnelle par rapport à celle des éditeurs de sites* web *les droits fondamentaux de la vie privée et de la protection des données à caractère personnel* » et que l'exploitant doit en conséquence assurer que cette activité « *satisfait aux exigences de la directive 95/46 pour que les garanties prévues par celle-ci puissent développer leur plein effet* » (§ 38).

Dès lors que cette étape était franchie, l'ensemble des droits reconnus à la personne par la directive devenait applicable au moteur de recherche, notamment le droit d'obtenir « *selon le cas, la rectification, l'effacement ou le verrouillage des données dont le traitement n'est pas conforme à la présente directive, notamment en raison du caractère incomplet ou inexact des données* », prévu par l'article 12, ainsi que le droit de « *s'opposer à tout moment, pour des raisons prépondérantes et légitimes tenant à sa situation particulière, à ce que des données la concernant fassent l'objet d'un traitement* », prévu par l'article 14. La CJUE a jugé qu'un moteur de recherche « *est susceptible d'affecter significativement les droits fondamentaux au respect de la vie privée et à la protection des données à caractère personnel lorsque la recherche à l'aide de ce moteur est effectuée à partir du nom d'une personne physique, dès lors que ledit traitement permet à tout internaute d'obtenir par la liste de résultats un aperçu structuré des informations relatives à cette personne trouvables sur Internet, qui touchent potentiellement à une multitude d'aspects de sa vie privée* » (§ 80). Dès lors, le seul intérêt économique du moteur de recherche ne peut suffire à justifier une ingérence de cette gravité, mais il y a lieu de prendre en compte « *l'intérêt légitime des internautes potentiellement intéressés à avoir accès* » à ces informations et de procéder à une pesée de cet intérêt et de celui de la personne concernée. En règle générale, l'intérêt de la personne concernée

doit prévaloir, mais l'équilibre peut dépendre de la nature de l'information et de sa sensibilité pour la vie privée ainsi que « *du rôle joué par cette personne dans la vie publique* », qui accroît l'intérêt du public à disposer de l'information (§ 81).

La CJUE donne enfin une sorte de « *mode d'emploi* » de la pesée des intérêts à opérer lorsqu'une personne exerce son droit d'opposition (article 12) ou d'effacement (article 14) à l'encontre d'un moteur de recherche. Selon son arrêt, qu'il est ici nécessaire de citer dans son intégralité : « *(…) Il convient notamment d'examiner si la personne concernée a un droit à ce que l'information en question relative à sa personne ne soit plus, au stade actuel, liée à son nom par une liste de résultats affichée à la suite d'une recherche effectuée à partir de son nom, sans pour autant que la constatation d'un tel droit présuppose que l'inclusion de l'information en question dans cette liste cause un préjudice à cette personne. Cette dernière pouvant, eu égard à ses droits fondamentaux au titre des articles 7 et 8 de la Charte, demander que l'information en question ne soit plus mise à la disposition du grand public du fait de son inclusion dans une telle liste de résultats, ces droits prévalent, en principe, non seulement sur l'intérêt économique de l'exploitant du moteur de recherche, mais également sur l'intérêt de ce public à accéder à ladite information lors d'une recherche portant sur le nom de cette personne. Cependant, tel ne serait pas le cas s'il apparaissait, pour des raisons particulières, telles que le rôle joué par ladite personne dans la vie publique, que l'ingérence dans ses droits fondamentaux est justifiée par l'intérêt prépondérant dudit public à avoir, du fait de cette inclusion, accès à l'information en question.* » (§ 99).

Dans la pesée des intérêts, la CJUE a ainsi clairement affirmé le principe selon lequel l'intérêt de la personne prévaut sur l'intérêt du moteur de recherche et des personnes souhaitant avoir accès à des informations sur celle-ci. L'équilibre ne se trouve inversé que si la personne joue un rôle tel dans la vie publique que l'intérêt du public à l'information devient prépondérant. La CJUE a donc consacré un large « *droit à l'oubli* » reposant sur le droit au déréférencement : toute personne a en principe le droit d'obtenir d'un moteur de recherche qu'il n'affiche pas certaines informations la concernant, même si ces informations ne lui sont pas préjudiciables. Cet arrêt témoigne de la force des principes fondamentaux définis par la directive n° 95/46/CE et de leur capacité à peser sur le fonctionnement d'un des acteurs majeurs de la société numérique contemporaine.

• *Un arrêt qui suscite des interrogations sur la conciliation à opérer entre droit à la vie privée et liberté d'expression*

L'arrêt *Google Spain c/ AEPD* est très protecteur de la vie privée des particuliers. Ses conséquences sur la liberté d'expression sont en revanche contestées. Jimmy Wales, le fondateur de l'encyclopédie en ligne *Wikipedia* a dénoncé l'arrêt comme instaurant « *l'une des censures les plus étendues jamais vues sur internet* »[302] et s'est inquiété de ses conséquences pour son propre site. La contribution de Winston J. Maxwell à cette étude[303] résume bien le point de vue anglo-saxon sur les effets

302. "*One of the most wide-sweeping internet censorship rulings that I've ever seen*" ; interview à la BBC le 14 mai 2014.
303. Voir p. 393.

« réfrigérants » que le droit au déréférencement pourrait avoir sur l'expression des opinions. Avant même l'arrêt de la CJUE, le concept de « droit à l'oubli » ne faisait d'ailleurs pas l'objet d'un consensus en Europe ; des archivistes et des historiens s'étaient notamment inquiétés des risques pour la recherche historique et la mémoire collective que comportaient certaines dispositions de la proposition de règlement.

La problématique de la conciliation entre droit à la vie privée et liberté d'expression n'est pas neuve. Le juge judiciaire français, sur le fondement de l'article 9 du code civil et la CEDH, sur le fondement des articles 8 et 10 de la convention, ont développé une jurisprudence abondante sur ce sujet, qui cherche le juste équilibre entre le droit de chacun au respect de sa vie privée et la liberté d'informer. Celui-ci se traduit par une nécessaire pesée, dans chaque espèce, de l'intérêt de l'information pour le public et de la sensibilité des informations en cause (les informations concernant la vie affective ou la santé étant considérées comme particulièrement sensibles) en tenant compte, le cas échéant, de ce que les faits ont été divulgués par l'intéressé lui-même.

Le droit de l'Union européenne relatif à la protection des données personnelles s'inscrit dans cette recherche d'équilibre. La directive n° 95/46/CE a prévu un régime particulier pour les traitements effectués aux seules fin de journalisme ou d'expression artistique ou littéraire : son article 9 dispose que les États prévoient pour ceux-ci des dérogations aux règles générales de la directive, « *dans la seule mesure où elles s'avèrent nécessaires pour concilier le droit à la vie privée avec les règles régissant la liberté d'expression* ». En France, l'article 67 de la loi du 6 janvier 1978, qui transpose cette disposition, ouvre de multiples dérogations dans le cadre de l'exercice à titre professionnel de l'activité de journaliste : les traitements de données mis en œuvre dans ce cadre ne sont ainsi soumis ni à la limitation de la durée de conservation, ni à l'interdiction du traitement des données sensibles, ni à l'obligation de déclaration à la CNIL, ni aux droits d'accès et de rectification. L'arrêt *Bodil Lindqvist* de la Cour de Luxembourg, tout en considérant que la mise en ligne d'informations relatives à des personnes sur un site internet constitue un traitement de données personnelles et entre donc dans le champ d'application de la directive, a jugé qu'il « *appartient aux autorités et aux juridictions nationales chargées d'appliquer la réglementation nationale transposant ladite directive d'assurer un juste équilibre des droits et intérêts en cause* », notamment au regard de la liberté d'expression garantie par l'article 10 de la convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales (CJCE, 6 novembre 2003, C-101/01). Le droit de l'Union européenne reconnaît donc que la liberté d'expression justifie des dérogations aux règles de protection des données personnelles, tout en laissant une importante marge de manœuvre aux États pour les définir.

L'arrêt *Google Spain* s'inscrit dans cette recherche d'équilibre mais en déplace cependant le curseur. Certes, il ne concerne que les moteurs de recherche et non les sites qui publient initialement ces informations, la CJUE ayant clairement affirmé que le référencement d'une information pouvait être contraire à la directive alors même que la publication de l'information sur le site était licite, notamment lorsqu'il s'agit d'un site de journalisme (§ 85 et § 88). Cependant, le

déréférencement affecte la liberté d'expression de l'éditeur du site en rendant l'information publiée moins accessible et en le ramenant ainsi à la situation antérieure à internet, où les informations relatives à une personne, publiées de manière licite sur différents supports, ne pouvaient pas être recoupées de manière instantanée et sans limitation dans le temps. L'arrêt *Google Spain* rétablit donc, dans une certaine mesure, l'équilibre entre liberté d'expression et droit à la vie privée qui prévalait avant l'essor d'internet et des moteurs de recherche. Cet équilibre n'était pas alors jugé attentatoire à la liberté d'expression, mais on a vu plus haut à quel point l'abondance d'informations disponibles sur les réseaux a rendu indispensable la visibilité de ces informations et, par suite, donné un rôle décisif à leur « fléchage » par le référencement sur une plateforme.

D'autres inquiétudes françaises quant au « droit à l'oubli » paraissent moins fondées. Le site *Wikipedia* ou les autres encyclopédies en ligne ne sont pas des moteurs de recherche ; en outre, elles ne traitent en principe que de personnalités participant à la vie publique, à propos desquelles la CJUE a rappelé le caractère prépondérant du droit du public à l'information. Quant aux archives, le dépôt légal des sites internet auprès de la BNF, prévu par l'article L. 131-2 du code du patrimoine, garantit aux futurs historiens l'accès à une masse d'informations très supérieure à tout ce qui a pu être collecté dans le passé ; l'arrêt *Google Spain* n'y porte pas atteinte, puisqu'il ne tend pas à modifier le contenu des sites mais seulement leur référencement. Enfin, il a parfois été avancé que l'arrêt *Google Spain* donnait aux moteurs de recherche un pouvoir trop important dans la sélection des informations devant être ou non effacées. C'est oublier que cette décision, qui incombe nécessairement au responsable de traitement, ne saurait être arbitraire : elle doit se faire dans le cadre défini par l'arrêt de la CJUE et est susceptible de recours devant l'autorité de contrôle ou la juridiction compétente. La définition de lignes directrices par les autorités de contrôle pourrait utilement compléter cet encadrement (cf. *infra* 3.2.1).

On ne peut enfin exclure que la jurisprudence *Google Spain* soit étendue aux réseaux sociaux et que sa portée en soit ainsi accrue. Un réseau social est en effet un traitement de données personnelles, puisqu'il permet la mise en ligne d'informations concernant des personnes ; même si les informations sont fournies par les utilisateurs, on pourrait considérer l'exploitant du réseau social comme le responsable du traitement, dans la mesure où il en détermine « *les finalités et les moyens* ». Dès lors, les droits d'effacement et d'opposition pourraient être exercés à son encontre. Si un raisonnement similaire à celui de *Google Spain* était retenu, les internautes disposeraient alors de larges possibilités d'obtenir l'effacement d'informations les concernant mises en ligne par des tiers ou par eux-mêmes, le consentement à un traitement de données pouvant être retiré.

Cependant, trois difficultés se présentent qui, si elles ne sont pas résolues, pourraient nuire à la mise en oeuvre efficace dû droit au déréférencement :

- Il importe que les éditeurs des sites dont le déréférencement est demandé soient en mesure de faire valoir leurs observations avant la décision de l'exploitant du moteur de recherche. Cet échange contradictoire est nécessaire pour que l'exploitant puisse procéder à la pesée des intérêts requise par l'arrêt *Google Spain*.

- Il est dans la logique de la directive n°95/46 que les exploitants de moteurs de recherche, qui sont les responsables du traitement des données, statuent sur les demandes de déréférencement, sous le contrôle de l'autorité de protection des données et du juge. Il faut cependant veiller à ce que ce pouvoir ne s'exerce pas de manière arbitraire.

- Le déréférencement risque d'être aisément contourné si les exploitants de moteur de recherche ne l'appliquent qu'à certaines versions linguistiques de leur site, ce qui ne serait pas conforme au champ d'application du droit de l'Union européenne.

Des propositions seront formulées dans la troisième partie pour remédier à ces difficultés.

La proposition de règlement procède à une rénovation justifiée des instruments de la protection des données, qui devrait être poussée encore plus loin

La proposition de règlement du 25 janvier 2012 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données[304] est destinée à se substituer à la directive n° 95/46/CE. Si elle n'a pas encore fait l'objet, au jour de la publication de cette étude, d'une position commune du Conseil, le Parlement européen en a adopté le 12 mars 2014 une version amendée, à une large majorité de 621 voix pour, 10 contre et 22 abstentions.

L'un des premiers enjeux de ce règlement est de mettre en place un corps de règles uniques dans l'ensemble de l'Union européenne, en lieu et place des lois nationales transposant l'actuelle directive. Ceci a des conséquences pour la répartition des compétences entre autorités nationales de protection des données et l'applicabilité des règles européennes aux acteurs établis hors de l'Union, qui seront examinées plus loin (cf. *infra* 2.4). On s'intéressera ici au fait que le règlement européen réaffirme les grands principes du cadre de protection des données personnelles, tout en en rénovant les instruments, comme le préconise le Conseil d'État dans cette étude. L'approche générale du règlement doit donc être soutenue ; on peut cependant estimer que les nouveaux énoncés des principes relatifs à la qualité des données sont parfois trop restrictifs, que la rénovation des instruments pourrait être poussée plus loin et que certaines dispositions sont inutilement détaillées ou porteuses d'insécurité juridique.

• *Une réaffirmation des principes, énoncée de manière restrictive.*

Les grands principes du cadre européen de la protection des données personnelles sont tous réaffirmés par la proposition de règlement. Les définitions des données à caractère personnel et des données sensibles sont maintenues à l'identique. Les principes relatifs à la qualité des données, renommés « *principes relatifs au traitement des données à caractère personnel* », sont repris presque sans changement, avec l'ajout d'un sixième principe, selon lequel la charge de la preuve

304. 2012/0011 (COD).

de la conformité d'un traitement au règlement incombe à son responsable[305]. Les listes des exceptions aux interdictions de traiter des données sensibles ou des données personnelles en l'absence du consentement de la personne[306] ne sont modifiées qu'à la marge.

On peut toutefois s'interroger sur la définition de certains principes, plus restrictive que dans la directive actuelle :

- S'agissant du principe de proportionnalité, alors que la directive disposait seulement que les données devaient être « *non excessives au regard des finalités pour lesquelles elles sont collectées et pour lesquelles elles sont traitées ultérieurement* », la proposition de règlement affirme qu'elles doivent être « *limitées au minimum nécessaire au regard des finalités pour lesquelles elles sont traitées* », ce qui invite l'autorité de protection des données à exercer un contrôle plus resserré[307] ; le principe est d'ailleurs dénommé principe de « *limitation des données au minimum* » ou de « *minimisation des données* ». Pour l'appréciation du respect de ce principe, la proposition de règlement impose en outre un nouveau test, consistant à s'assurer que « *les finalités du traitement ne peuvent pas être atteintes par le traitement d'informations ne contenant pas des données à caractère personnel* ».

- S'agissant du principe de finalités déterminées, la disposition selon laquelle un traitement ultérieur à des fins historiques, statistiques ou scientifiques n'est pas réputé incompatible avec les finalités initiales ne figure plus dans la proposition de règlement.

Ces définitions restrictives sont susceptibles d'amoindrir la sécurité juridique des usages du *Big Data* à caractère statistique, qui reposent notamment sur la réutilisation des données à d'autres fins que celles pour lesquelles elles avaient été

305. Le texte voté par le Parlement européen en ajoute deux autres : le principe d'effectivité, selon lequel les données doivent être traitées « *d'une manière qui permettre à la personne d'exercer effectivement ses droits* », et le principe d'intégrité, en vertu duquel elles doivent être « *traitées de façon à les protéger contre le traitement non autorisé ou illicite et contre la perte, la destruction ou les dégâts d'origine accidentelle, à l'aide de mesures techniques ou organisationnelles appropriées* ».

306. Exécution d'un contrat, respect d'une obligation légale, sauvegarde des intérêts vitaux de la personne concernée, exécution d'une mission d'intérêt général, intérêt légitime du responsable du traitement.

307. Parallèlement à la proposition de règlement, la Commission a adopté une proposition de directive relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données ; le Parlement européen s'est également prononcé sur cette directive le 12 mars 2014. Alors que pour la directive, la proposition de la Commission s'en tenait à une formulation souple du principe de proportionnalité (données « *adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont traitées* »), le Parlement européen a retenu la même rédaction stricte que pour la proposition de règlement (données « *adéquates, pertinentes et limitées au minimum nécessaire au regard des finalités pour lesquelles elles sont traitées* »).

collectées. Sur le plan des symboles, l'affichage d'un principe de « minimisation des données », même si elle ne constitue qu'un changement de degré par rapport à l'actuel principe de proportionnalité, risque de constituer un signal négatif à l'égard du développement du *Big Data*.

• *Une transformation des instruments qui pourrait être poussée encore plus loin*

Plusieurs mesures vont dans le sens d'une rénovation des instruments de la protection.

- L'obligation de déclaration à l'autorité de contrôle est supprimée et remplacée par une obligation de consultation de celle-ci pour les seuls traitements présentant des risques particuliers pour les droits et libertés des personnes concernées (article 34 de la proposition).

- La désignation d'un délégué à la protection des données (DPD) devient obligatoire pour tous les organismes publics et pour les traitements des entreprises privées d'une certaine taille ou dont les activités de base consistent en des traitements impliquant un suivi régulier et systématique des personnes concernées[308] (article 35).

- Plusieurs obligations tendent à renforcer la prise en compte par le responsable de traitement des risques de son activité et à vérifier sa capacité à rendre des comptes (son « *accountability* ») : obligation de prendre en compte les exigences du règlement dès la conception d'un traitement de données, dite de « protection des données dès la conception » ou, en anglais, « *privacy by design* »[309] (article 23) ; obligation, en cas de désignation d'un sous-traitant, de s'assurer de sa capacité à assurer la conformité du traitement au règlement (article 26) ; obligation de conserver une documentation retraçant tous les traitements de données et permettant de s'assurer de leur conformité[310] (article 28) ; obligation de notifier à l'autorité de contrôle et à la personne concernée les violations de données à caractère personnel, qui ne s'applique aujourd'hui qu'aux opérateurs

308. La proposition de la Commission fixait un seuil de 250 salariés. Le texte voté par le Parlement européen exprime le seuil en nombre de personnes concernées par le traitement (5 000 sur une période de douze mois consécutifs). Il ajoute en outre une nouvelle catégorie de personnes soumises à l'obligation de désigner un DPD : celles dont les activités de base consistent à traiter des données sensibles (ce qui couvre notamment tous les acteurs traitant des données de santé), des données de localisation ou des données relatives à des enfants ou des employés.

309. Le Parlement européen a ajouté que la protection des données dès la conception devrait être une « *condition préalable aux offres de marchés publics* ».

310. La documentation doit notamment comporter les finalités du traitement, la description des catégories de personnes concernées et des catégories de données s'y rapportant ainsi que les catégories de destinataires des données. On retrouve ici le contenu des déclarations à l'autorité de contrôle, obligatoires dans le cadre juridique actuel (article 30 de la loi du 6 janvier 1978) ; au lieu d'être communiquées systématiquement à l'autorité de contrôle, ces informations doivent être tenues à sa disposition.

de communications électroniques et qui est étendue à tous les responsables de traitement (articles 31 et 32) ; obligation de réaliser une analyse d'impact pour les traitements présentant des risques particuliers (article 33)[311].

- Les droits des personnes sont renforcés de façon à en faciliter la mise en œuvre. Les droits d'information, d'accès, de rectification et d'opposition sont repris dans des termes très proches de ceux de la directive n° 95/46/CE. Le règlement précise cependant, dans un article 12 intitulé « *Procédures et mécanismes prévus pour l'exercice des droits de la personne concernée* », que le responsable de traitement doit mettre en place des mécanismes facilitant l'exercice de ces droits, notamment en permettant de faire la demande par voie électronique, et doit informer les personnes des suites données à leurs demandes et, le cas échéant, des voies de recours, dans un délai d'un mois. Le droit d'accès est complété par un « *droit à la portabilité des données* », impliquant la possibilité pour la personne d'obtenir la communication des données la concernant dans un « *format structuré et couramment utilisé* » et, lorsque les données ont été initialement communiquées par la personne, de les réutiliser et de les transmettre à d'autres personnes (ce qui tend à garantir la possibilité de changer de prestataire de service)[312]. Est ajouté un droit à l'effacement, renommé *droit à l'oubli* par la proposition de règlement (cette expression n'a pas été maintenue par le Parlement européen).

- Le texte voté par le Parlement européen introduit une obligation de normalisation de la politique de protection des données appliquée par chaque responsable de traitement, qui doit la présenter par des pictogrammes définis par le règlement, dans un format lisible par la machine. Cette disposition est similaire à la proposition de standardisation des « *privacy policies* » formulée par Lawrence Lessig et pourrait permettre un progrès important dans leur lisibilité par les personnes concernées.

- Alors que la directive laissait le soin à chaque État de prévoir des sanctions appropriées, la proposition de règlement confère aux autorités de contrôle le pouvoir d'infliger des sanctions administratives, pouvant aller jusqu'à 1 million d'euros ou, pour une entreprise, 2 % de son chiffre d'affaires annuel mondial[313].

Ces dispositions tendent à renforcer le contrôle en continu de la conformité des traitements au cadre juridique de la protection des données personnelles. Elles permettent une meilleure adéquation des obligations aux risques représentés par les traitements : la plupart des responsables de traitement seront désormais dispensés de toute obligation déclarative ; les responsables des traitements présentant des risques particuliers seront au contraire soumis à de fortes obligations. La fixation des sanctions à un niveau susceptible de dissuader les plus importants acteurs de l'économie numérique répond à une nécessité.

---

311. Le Parlement européen a complété cette obligation d'étude d'impact par une obligation d'examen de la conformité, dans les deux ans suivant la réalisation de l'étude d'impact (article 33 *bis*).

312. Le texte voté par le Parlement européen ne fait plus de la portabilité des données un droit distinct, mais une composante du droit d'accès.

313. Le Parlement européen a porté ces plafonds à 100 millions d'euros ou 5 % du chiffre d'affaires annuel mondial.

D'autres voies de réforme des instruments de protection, dans le sens indiqué plus haut (cf. *supra* 2.1.3), pourraient être explorées plus avant, notamment en ce qui concerne les technologies de renforcement de la vie privée, la définition d'une « chaîne de responsabilités » des acteurs impliqués dans le traitement des données, l'attention particulière portée à la circulation des données personnelles, le développement de la certification et de la corégulation ; les propositions correspondantes du Conseil d'État seront développées plus loin (cf. *infra* 3.3.1).

• *Des dispositions parfois inutilement détaillées ou porteuses d'insécurité juridique*

La directive n° 95/46/CE compte 34 articles et 72 considérants. La proposition de règlement comporte 91 articles et 139 considérants. Les auteurs du règlement ont sans doute voulu remédier au manque d'effectivité du cadre actuel par la définition précise des obligations des responsables de traitement. Toutefois, ce parti expose le règlement à un risque d'obsolescence rapide : depuis l'adoption de la proposition de règlement par la Commission, deux ans et demi se sont déjà écoulés, au cours desquels les technologies et les usages du numérique ont poursuivi leur évolution ; le règlement n'est pas encore adopté et il ne deviendra applicable que deux ans après sa publication, soit en 2017 dans le meilleur des cas. Plus les dispositions du règlement entrent dans les modalités d'application et dans la prise en compte du contexte technologique, plus le risque d'une diminution de leur pertinence au fil du temps est élevé.

On peut en particulier s'interroger sur la nécessité de fixer dans le règlement toutes les modalités de l'obligation de normalisation des politiques d'utilisation des données personnelles, jusqu'à inscrire les pictogrammes en annexe du texte adopté par le Parlement européen et le Conseil. Il en va de même pour la définition de toutes les rubriques de l'analyse d'impact, de toutes les tâches du délégué à la protection des données (et même de ses qualifications professionnelles dans un considérant voté par le Parlement européen) et de toutes les clauses des relations entre le responsable de traitement et son sous-traitant. De telles dispositions pourraient être renvoyées à un acte délégué de la Commission, plus aisément modifiable qu'un règlement du Parlement européen et du Conseil, voire à des instruments de droit souple adoptés par le Comité européen de la protection des données, appelé à remplacer le G29 avec des prérogatives accrues, ou par les acteurs professionnels dans le cadre de codes de conduite.

L'imprécision d'autres dispositions pourrait être source d'insécurité juridique. Il en va ainsi par exemple du champ d'application de l'obligation de consultation préalable des autorités de contrôle. L'article 34 prévoit deux cas dans lesquels l'autorité de contrôle doit être consultée avant la mise en œuvre du traitement : lorsqu'une analyse d'impact « *indique que les traitements sont, du fait de leur nature, de leur portée ou de leurs finalités, susceptibles de présenter un degré élevé de risques particuliers* » ou lorsque le traitement appartient à une des catégories dont l'autorité nationale de contrôle a estimé qu'elle présentait des risques particuliers. Le fait qu'une obligation de consultation préalable, lourdement sanctionnée en

cas de manquement[314], dépende de l'évaluation du risque à l'issue de l'analyse d'impact est porteur d'une forte insécurité juridique ; il reviendrait au responsable de traitement, à l'issue de l'analyse d'impact, de déterminer si le degré de risque justifie la consultation préalable, au risque d'être sanctionné s'il sous-estime ce risque et qu'il est désavoué, à l'occasion d'un contrôle, par l'autorité de protection. Dans le texte adopté le 12 mars 2014, le Parlement européen a abandonné l'obligation de consultation préalable de l'autorité de contrôle, qui devient une obligation de consultation du DPD, sauf lorsque le responsable du traitement n'a pas désigné de DPD. Mais le système défini repose sur une architecture complexe, avec en premier lieu une « *analyse du risque* » pouvant dans certains cas nécessiter une « *analyse d'impact »*, puis, si le degré de risque est élevé, une consultation du DPD, et ce, alors même que le DPD doit être associé à la procédure d'analyse d'impact… S'il est légitime de définir de fortes obligations pour les traitements présentant des risques particuliers d'atteinte à la vie privée et à la protection des données personnelles, le champ d'application de ces obligations et leur teneur doivent être définis en termes clairs. Les incertitudes dont est entaché le texte actuel sont nuisibles à la protection effective de ces droits fondamentaux et au développement de l'économie numérique européenne, dont les acteurs doivent connaître les obligations qui leur incombent. Elles pourraient même être constitutives d'une méconnaissance du principe général du droit de l'Union européenne de sécurité juridique, en vertu duquel « *la législation communautaire doit être certaine et son application prévisible pour les justiciables* »[315].

Ces difficultés ne remettent pas en cause la pertinence de l'approche générale du règlement. Ne portant pas sur les éléments centraux de son architecture, elles sont de nature à être corrigées d'ici l'adoption définitive du texte.

2.1.5. La surveillance des communications par les pouvoirs publics présente des enjeux spécifiques et appelle des réponses adaptées

Les principes de la surveillance des communications par les pouvoirs publics ont été fixés par la loi du 10 juillet 1991. Celle-ci a réaffirmé le secret des communications et n'a permis d'y porter atteinte que dans deux hypothèses, sur décision de l'autorité judiciaire ou, « *à titre exceptionnel* » et pour des finalités définies par la loi, sur décision du Premier ministre et sous le contrôle de la Commission nationale de contrôle des interceptions de sécurité (CNCIS). Cependant, depuis cette date, les pratiques de surveillance des communications par les pouvoirs publics et leur contexte ont profondément évolué, suscitant d'importants débats sur leur place

314. L'article 79.6 de la proposition classe l'absence de consultation préalable, lorsqu'elle est requise, parmi les infractions les plus lourdement sanctionnées (maximum d'un million d'euros ou de 2 % du chiffre d'affaires mondial annuel).

315. Cf. par exemple CJCE 15 déc. 1987, *Irlande c/ Commission*, C-325/85. Pour une analyse générale, J.-P. Puissochet et H. Legal, « Le principe de sécurité juridique dans la jurisprudence de la Cour de justice des Communautés européennes », *Cahiers du Conseil constitutionnel*, n° 11, décembre 2001.

et les garanties qui doivent les entourer. L'essor des communications électroniques et des capacités de stockage et d'analyse des données a démultiplié les possibilités d'interception[316]. Les deux derniers livres blancs sur la défense ont fait de la collecte de renseignements par cette voie l'une des priorités de la politique de sécurité nationale de la France, qui s'est traduite par une forte augmentation des moyens matériels des services. Le débat est également nourri par des facteurs exogènes à la France : l'arrêt *Digital Rights Ireland* du 8 avril 2014 de la CJUE a remis en cause le cadre européen de la conservation des données ; les révélations de ce qu'il est convenu d'appeler « l'affaire *Prism* » ont, partout dans le monde, porté ces sujets au premier plan du débat public.

Depuis la loi du 10 juillet 1991, le législateur a procédé en la matière par extensions successives : création d'une procédure de réquisition administrative des métadonnées par la loi du 23 janvier 2006 ; pérennisation et extension des finalités de cette procédure, ainsi que des services habilités à la demander, par la loi du 18 décembre 2013. Il apparaît nécessaire aujourd'hui de procéder à un réexamen global du cadre juridique de la surveillance des communications, dans le but de préserver la capacité de notre pays à protéger sa sécurité nationale tout en apportant l'ensemble des garanties nécessaires à la protection des droits fondamentaux.

La collecte de renseignement par la surveillance des communications électroniques est un élément essentiel de la stratégie de défense et de sécurité de la France

La surveillance des communications par les pouvoirs publics est l'un des instruments d'une responsabilité éminente de l'État, celle d'assurer la protection de la sécurité de la population et la défense des intérêts fondamentaux de la Nation[317]. Si les interceptions judiciaires s'inscrivent pleinement dans les missions de la police judiciaire, les interceptions administratives relèvent d'une démarche de prévention de la criminalité organisée, du terrorisme et des autres menaces contre la sécurité nationale[318]. À la différence des missions classiques de la police, qui consistent à rechercher les auteurs d'infractions déjà commises ou à lutter contre des menaces

316. Comme dans la première partie, on emploie ici le terme d'« *interceptions* » au sens large, en y incluant les interceptions du contenu des communications et la collecte des métadonnées.

317. Que l'article 410-1 du code pénal définit ainsi : « *Les intérêts fondamentaux de la nation s'entendent au sens du présent titre de son indépendance, de l'intégrité de son territoire, de sa sécurité, de la forme républicaine de ses institutions, des moyens de sa défense et de sa diplomatie, de la sauvegarde de sa population en France et à l'étranger, de l'équilibre de son milieu naturel et de son environnement et des éléments essentiels de son potentiel scientifique et économique et de son patrimoine culturel.* »

318. Selon l'article L. 1111-1 du code de la défense, « *la stratégie de sécurité nationale a pour objet d'identifier l'ensemble des menaces et des risques susceptibles d'affecter la vie de la Nation, notamment en ce qui concerne la protection de la population, l'intégrité du territoire et la permanence des institutions de la République, et de déterminer les réponses que les pouvoirs publics doivent y apporter* ». Au sein de la stratégie de sécurité nationale, la politique de défense a pour objet de protéger le territoire et la population contre les agressions armées.

avérées pour l'ordre public, l'action des services de renseignement peut porter sur des informations dont l'utilité n'est qu'éventuelle au moment de leur collecte et qui seront conservées en vue de recoupements futurs[319].

Deux constantes se dégagent de la politique de la France au cours des dernières années : le constat d'une plus grande diversité des menaces contre la sécurité nationale ; la nécessité pour y répondre d'accroître les moyens des services de renseignement, notamment les moyens d'interception des communications électroniques. Les deux derniers livres blancs sur la défense nationale, publiés en 2008 et en 2013, ont souligné « *l'incertitude stratégique* » liée à la mondialisation, à l'augmentation des inégalités, aux tensions sur les ressources naturelles, au déplacement progressif du centre de gravité stratégique vers l'Asie, à l'augmentation des dépenses militaires dans le monde, à la privatisation de la violence armée ou à l'irrésolution de nombreux conflits armés : les menaces contre la sécurité nationale sont plus diverses et moins prévisibles que dans le passé. Ils ont tous deux mis en exergue, parmi ces menaces, celles résultant du terrorisme et de la criminalité organisée. En raison de divers facteurs, dont son degré d'engagement dans des opérations armées extérieures et la place persistante du terrorisme séparatiste, la France apparaît comme l'un des pays européens les plus exposés à la menace terroriste, qui peut frapper soit ses intérêts et ses ressortissants à l'étranger, soit sur son territoire. En 2012, selon Europol, plus de la moitié des attaques terroristes qui ont abouti, échoué ou ont été déjouées et plus du tiers des arrestations liées au terrorisme en Europe concernaient notre territoire[320].

Face à ces menaces diverses et difficilement prévisibles, les deux derniers livres blancs ont fait des fonctions d'analyse et de connaissance l'une des premières priorités de la stratégie de sécurité nationale. Ces choix ont été inscrits dans les lois de programmation militaire du 29 juillet 2009 et du 18 décembre 2013, votées sous deux majorités politiques différentes. Au sein d'un budget de défense globalement stable et d'effectifs des armées en réduction, les services de renseignement bénéficient de moyens humains et financiers en forte augmentation. Le « *renseignement d'origine électromagnétique* », terminologie militaire pour désigner l'interception des communications électroniques, est qualifié par le rapport annexé à la loi du 18 décembre 2013 de « *composante essentielle du dispositif d'ensemble* ».

Il faut ajouter que le renseignement sert non seulement à déjouer les menaces directes contre notre territoire ou notre population, mais aussi à accompagner l'engagement de la France au service de la sécurité collective. Il contribue au bon

319. Cette différence se manifeste dans les différences de condition d'inscription dans les fichiers. Pour qu'une personne soit inscrite comme « *mise en cause* » dans les fichiers de police tels que le fichier « *traitement d'antécédents judiciaires* » (TAJ) ou le fichier national automatisé des empreintes génétiques (FNAEG), il doit exister des « *indices graves ou concordants* » qu'elles ont participé à la commission d'une infraction. Pour les fichiers de renseignement, le Conseil d'État a jugé que les données devaient seulement être « *pertinentes au regard des finalités poursuivies* » (CE, 16 avril 2010, *Association Aides et autres*, n° 320196, Rec. p. 117.

320. Europol, *EU Terrorism Situation and Trend Report*, 2013 : 125 attaques sur 219 et 186 arrestations sur 537.

déroulement des missions de maintien de la paix auxquelles participe la France ainsi qu'à la lutte contre la prolifération des armes nucléaires, biologiques et chimiques.

L'arrêt Digital Rights Ireland *de la CJUE a remis en cause le cadre européen de la conservation des données de communications électroniques et son incidence sur les législations nationales fait l'objet d'interrogations.*

• *Le cadre européen de la conservation des données de communications électroniques*

La directive n° 2002/58/CE, dite *vie privée et communications électroniques*, énonce un principe de confidentialité, qui interdit « *à toute autre personne que les utilisateurs d'écouter, d'intercepter, de stocker les communications et les données relatives au trafic y afférentes* » (article 5.1). L'article 15.1 ne permet aux États membres d'adopter des lois limitant la portée de ce principe que dans la mesure où une telle limitation « *constitue une mesure nécessaire, appropriée et proportionnée, au sein d'une société démocratique, pour sauvegarder la sécurité nationale — c'est-à-dire la sûreté de l'État — la défense et la sécurité publique, ou assurer la prévention, la recherche, la détection et la poursuite d'infractions pénales ou d'utilisations non autorisées du système de communications électroniques* » ; cette rédaction est directement inspirée par la jurisprudence de la CEDH sur la surveillance des communications par les États (cf. l'encadré au 1.3.3). L'article 15.1 permet en particulier aux États d'adopter « *des mesures législatives prévoyant la conservation de données pendant une durée limitée* ». Le considérant 11 fait ressortir que l'intention des auteurs de la directive a été de ne pas traiter d'une question qui touchait à des domaines non régis par le droit communautaire, tels que la protection de la sécurité publique, de la défense et de la sûreté de l'État, et de seulement renvoyer à l'application de la jurisprudence de la CEDH.

Dans un contexte marqué par les attentats de Madrid, le 11 mars 2004, et de Londres en juillet 2005, les institutions de l'Union européenne ont adopté la directive n° 2006/24/CE du 15 mars 2006, dite « *directive relative à la conservation des données* ». Celle-ci a pour objet « *d'harmoniser les dispositions des États membres relatives aux obligations des fournisseurs de services de communications électroniques accessibles au public ou de réseaux publics de communications en matière de conservation de certaines données qui sont générées ou traitées par ces fournisseurs, en vue de garantir la disponibilité de ces données à des fins de recherche, de détection et de poursuite d'infractions graves telles qu'elles sont définies par chaque État membre dans son droit interne* » (article 1.1). Elle définit les catégories de données conservées, qui ne portent que sur des métadonnées[321] et pas sur le contenu des communications (et notamment pas sur le contenu de sites visités sur internet), et prévoit que les durées de conservation fixées par les États doivent être comprises entre six mois et deux ans.

---

321. L'article 5, très détaillé, prévoit notamment la conservation des identifiants (numéros de téléphone et adresses IP) et des identités de l'appelant et de l'appelé, de la date, de l'heure et de la durée des communications, de données relatives aux équipements utilisés et de données de localisation pour les téléphones mobiles.

• *L'arrêt* Digital Rights Ireland *et* Seitleinger *de la CJUE*

La CJUE a été saisie de questions concernant la conformité de cette directive à la Charte des droits fondamentaux de l'Union européenne et notamment à ses articles 7, 8 et 11 relatifs au droit à la vie privée, au droit à la protection des données personnelles et à la liberté d'expression, dans le cadre de deux renvois préjudiciels effectués par la *High Court* irlandaise et la Cour constitutionnelle autrichienne. Par un arrêt du 8 avril 2014[322], la Grande chambre de la CJUE a déclaré la directive invalide en raison de la méconnaissance des articles 7 et 8 de la Charte.

L'arrêt *Digital Right Ireland* et *Seitlinger* de la CJUE, qui sera dénommé par commodité « *Digital Rights* », se prononce en premier lieu sur la sensibilité des métadonnées et sur l'ampleur de l'ingérence dans les droits à la vie privée et à la protection des données personnelles que représente leur conservation systématique. La Cour estime que « *ces données, prises dans leur ensemble, sont susceptibles de permettre de tirer des conclusions très précises concernant la vie privée des personnes dont les données ont été conservées, telles que les habitudes de la vie quotidienne, les lieux de séjour permanents ou temporaires, les déplacements journaliers ou autres, les activités exercées, les relations sociales de ces personnes et les milieux sociaux fréquentés par celles-ci* » (§ 27). Elle juge que « *l'ingérence que comporte la directive 2006/24 dans les droits fondamentaux consacrés aux articles 7 et 8 de la Charte s'avère (…) d'une vaste ampleur et qu'elle doit être considérée comme particulièrement grave* » et que « *la circonstance que la conservation des données et l'utilisation ultérieure de celles-ci sont effectuées sans que l'abonné ou l'utilisateur inscrit en soient informés est susceptible de générer dans l'esprit des personnes concernées (…) le sentiment que leur vie privée fait l'objet d'une surveillance constante* » (§ 37). Cette motivation diverge donc de celle de la décision n° 2005-532 DC du 19 janvier 2006 du Conseil constitutionnel, rendue sur la loi relative à la lutte contre le terrorisme, qui a instauré le cadre français de la réquisition administrative des métadonnées : le Conseil constitutionnel avait relevé que la disposition litigieuse « *se borne à instaurer une procédure de réquisition de données techniques* » (§ 8) ; le commentaire publié sur le site du Conseil constitutionnel indiquait que la réquisition de ces données techniques était moins attentatoire au respect de la vie privée que les interceptions de sécurité, qui portent sur le contenu même des communications.

Constatant l'existence d'une ingérence, la CJUE se fonde ensuite sur l'article 52 de la Charte, selon lequel les limitations de l'exercice d'un droit fondamental doivent être justifiées par des objectifs d'intérêt général reconnus par le droit de l'Union et nécessaires pour atteindre ces objectifs[323]. Elle reconnaît que la lutte contre le terrorisme et contre la criminalité organisée sont des buts d'intérêt général.

---

322. *Digital Rights Ireland et al.* et *Michael Seitlinger et al.*, C-293/12 et C-594/12.

323. Article 52.1 : « *Toute limitation de l'exercice des droits et libertés reconnus par la présente Charte doit être prévue par la loi et respecter le contenu essentiel desdits droits et libertés. Dans le respect du principe de proportionnalité, des limitations ne peuvent être apportées que si elles sont nécessaires et répondent effectivement à des objectifs d'intérêt général reconnus par l'Union ou au besoin de protection des droits et libertés d'autrui.* »

Elle estime que si le législateur de l'Union dispose d'un pouvoir d'appréciation pour choisir les moyens permettant d'atteindre de tels buts d'intérêt général, ce pouvoir d'appréciation peut être restreint en raison de la nature et de la gravité de l'ingérence. Elle juge qu'en l'espèce, « *compte tenu, d'une part, du rôle important que joue la protection des données à caractère personnel au regard du droit fondamental au respect de la vie privée et, d'autre part, de l'ampleur et de la gravité de l'ingérence dans ce droit que comporte la directive 2006/24, le pouvoir d'appréciation du législateur de l'Union s'avère réduit de sorte qu'il convient de procéder à un contrôle strict* » (§ 48).

Dans le cadre de ce contrôle strict de proportionnalité, trois éléments sont pris en compte par la Cour pour juger que les articles 7 et 8 de la Charte sont méconnus :

- le fait que la directive « *couvre de manière généralisée toute personne et tous les moyens de communication électronique ainsi que l'ensemble des données relatives au trafic sans qu'aucune différenciation, limitation ni exception soient opérées en fonction de l'objectif de lutte contre les infractions graves* » (§ 57) ;

- le fait qu'elle ne « *prévoit aucun critère objectif permettant de délimiter l'accès des autorités nationales compétentes aux données et leur utilisation ultérieure* », renvoyant entièrement sur ce point aux législations nationales (§ 60) ;

- le fait que la durée de conservation soit fixée sans tenir compte de l'utilité de la conservation par rapport aux objectifs poursuivis (§ 63 et 64).

C'est au vu de ces trois griefs que la Cour juge disproportionnée l'atteinte aux droits à la vie privée et à la protection des données personnelles (§ 65). Elle relève, en outre, que la directive ne prévoit pas de garanties suffisantes quant à la sécurité des données conservées et qu'elle n'impose pas la conservation sur le territoire de l'Union, ce qui ne permet pas de garantir le contrôle par une autorité indépendante de protection des données personnelles, prévu par l'article 8.3 de la Charte.

• *Les implications de l'arrêt*

L'arrêt *Digital Rights Ireland*, dont la Cour n'a pas différé les effets[324], soulève deux questions : celle de la possibilité de continuer à appliquer les législations nationales sur la conservation des données et celle du cadre qui devrait être défini pour se substituer à la directive n° 2006/24/CE. Les deux questions procèdent en réalité d'une même interrogation sur l'interprétation de l'arrêt. De manière schématique, deux lectures peuvent en être faites : celle d'une condamnation de l'insuffisance des garanties prévues par la directive ; celle d'une condamnation de tout système de conservation générale des métadonnées, quel qu'il soit.

Avant d'en venir à ces deux lectures, une question préalable doit être évoquée, celle de l'applicabilité de la Charte des droits fondamentaux de l'Union européenne

324. Les conclusions de l'avocat général Pedro Cruz Villalon, qui préconisait, en raison de la nature des buts de la directive, de suspendre les effets du constat d'invalidité jusqu'à ce que le législateur de l'Union prenne les mesures nécessaires pour y remédier, n'ont pas été suivies sur ce point, sans que la Cour motive ce choix.

aux législations nationales, à la suite de l'invalidation de la directive n° 2006/24/CE. L'article 51 de la Charte dispose qu'elle s'applique aux États membres « *uniquement lorsqu'ils mettent en œuvre le droit de l'Union* » ; selon la CJUE, les États doivent respecter les droits fondamentaux garantis par la Charte dès lors que leur action « *entre dans le champ d'application du droit de l'Union* » (cf. par exemple, Gde Ch., 26 février 2013, *Åklagaren c/ Hans Åkerberg Fransson*, C-617/10). Or, l'invalidation de la directive n° 2006/24/CE conduit à s'interroger sur l'existence d'actes de droit de l'Union applicables à la conservation des métadonnées par les opérateurs de communications électroniques et à leur utilisation à des fins de sécurité nationale ou de police judiciaire. En effet, tant la directive n° 95/46/CE que la directive n° 2002/58/CE excluent de leur champ la matière pénale et les traitements ayant pour objet la sécurité publique, la défense et la sûreté de l'État. Et l'existence de ces actes, mettant en œuvre le droit de l'Union, est une condition d'application de la Charte.

La directive n° 2002/58/CE est cependant ambigue à cet égard : si son article 1.3 restreint son champ d'application, son article 15.1 dispose que les États ne peuvent déroger aux droits garantis par la directive pour les finalités énumérées ci-dessus que s'il s'agit de mesures nécessaires et proportionnées, prises dans le respect des « *principes généraux du droit communautaire* ». Il traite en particulier de la conservation des données, en prévoyant que « *les États membres peuvent, entre autres, adopter des mesures législatives prévoyant la conservation de données pendant une durée limitée lorsque cela est justifié* » par l'une des finalités énumérées ci-dessus. Il est donc possible de soutenir que la directive n° 2002/58/CE régit les législations des États relatives à la conservation des métadonnées. Les usages des métadonnées en matière de sécurité nationale échappent au champ d'application du droit de l'Union, mais la conservation porte atteinte par elle-même, indépendamment de l'usage, aux droits garantis par la directive, puisque l'article 5 impose en principe l'effacement des données. En outre, si la proposition de directive relative à la protection des données personnelles en matière pénale était adoptée, les traitements de données personnelles à des fins de police judiciaire entreraient pleinement dans le champ du droit de l'Union européenne. Dès lors, en raison de l'ambiguïté du champ d'application de la directive n° 2002/58/CE, la question de la conformité de la législation nationale à la Charte des droits fondamentaux de l'Union européenne, telle qu'elle a été interprétée par la CJUE dans l'arrêt *Digital Rights Ireland*, reste posée.

La première interprétation de cet arrêt peut se fonder sur le fait que la Cour a fait masse de trois éléments pour juger que le principe de proportionnalité était méconnu, et que le second avait trait à l'absence de toute précision sur les conditions d'accès des États aux métadonnées conservées par les opérateurs. Selon cette interprétation, si la directive avait fixé des garanties concernant l'accès, l'appréciation de la Cour aurait peut-être été différente. Elle aurait également pu être influencée par l'existence de restrictions concernant la conservation, par exemple une durée maximale plus courte que celle de deux ans fixée par la directive. Les conclusions de l'avocat général peuvent conforter une telle interprétation. L'avocat général déplorait le fait que la directive n'ait défini ni la

nature des infractions pouvant justifier l'accès aux métadonnées, ni les autorités pouvant obtenir cet accès, ni les garanties relatives à l'effacement des données par les autorités après leur utilisation et à l'information des personnes concernées (§ 125 à 129 des conclusions). Il relevait aussi qu'il y avait une différence entre une durée de conservation se mesurant en mois et une durée se mesurant en années (§ 148). Cependant, si la Cour est parvenue à la même solution que l'avocat général, la construction de son raisonnement est assez différente, et il n'est donc pas évident que les conclusions permettent d'éclairer la portée de l'arrêt sur la condamnation du système de conservation en tant que tel.

La seconde interprétation se fonde en premier lieu sur ce que deux des trois éléments pris en compte par la Cour pour juger que le principe de proportionnalité est méconnu tiennent au caractère général et indiscriminé de la conservation : dans le premier élément, la Cour critique le fait que les métadonnées de tous les utilisateurs des communications soient collectées, indépendamment de l'existence d'un soupçon quant à la participation à une infraction grave ; dans le troisième élément, c'est le fait que la durée de conservation soit fixée de manière indiscriminée qui est contesté. C'est donc le caractère systématique et uniformément durable de la conservation des métadonnées qui est en cause. En second lieu, l'arrêt qualifie sévèrement la conservation systématique des métadonnées, en y voyant une « *ingérence particulièrement grave* » dans les droits garantis par les articles 7 et 8 de la Charte, l'absence d'information des intéressés étant en outre « *susceptible de générer dans l'esprit des personnes concernées (…) le sentiment que leur vie privée fait l'objet d'une surveillance constante* ». Si la Cour admet que la conservation préventive des données poursuit un but d'intérêt général, elle juge que l'ingérence ne peut être admise que si elle est proportionnée. À l'issue de son contrôle de proportionnalité, elle conclut que la directive « *comporte une ingérence dans ces droits fondamentaux d'une vaste ampleur et d'une gravité particulière dans l'ordre juridique de l'Union sans qu'une telle ingérence soit précisément encadrée par des dispositions permettant de garantir qu'elle est effectivement limitée au strict nécessaire* » (§ 65). On peut donc en déduire que l'ingérence résultant d'un système de conservation systématique peut difficilement être considérée comme « *limitée au strict nécessaire* ».

Si cette seconde interprétation devait être retenue, les lois nationales, telles que la loi française, qui prévoient la conservation systématique des métadonnées par les opérateurs, ne pourraient – sous réserve de la levée de l'ambiguïté exposée ci-dessus sur l'applicabilité du droit de l'Union européenne – être maintenues en l'état. Si elle s'avérait nécessaire, la mise en conformité de la législation nationale avec l'arrêt *Digital Rights Ireland* devrait se faire indépendamment du choix des institutions de l'Union européenne d'adopter, ou non, une nouvelle directive se substituant à la directive n° 2006/24/CE. À ce stade, la Commission européenne n'a d'ailleurs pas indiqué les suites qu'elle comptait donner à cet arrêt et elle a seulement annoncé qu'elle allait « *analyser attentivement le verdict et ses implications* »[325].

325. Communiqué du 8 avril 2014 de Cecilia Malmström, commissaire aux affaires intérieures.

« L'affaire Prism » a suscité d'importants débats sur les programmes gouvernementaux de surveillance des communications électroniques

Les révélations d'Edward Snowden ont débuté par deux articles du *Washington Post* et du *Guardian* publiés le 5 juin 2013, dévoilant l'existence d'un programme de collecte systématique des métadonnées des appels téléphoniques (notamment les numéros appelés et la durée de ces appels) passés aux États-Unis ou depuis les États-Unis vers l'étranger. Elles se sont ensuite égrenées au fil des mois suivants, mettant en avant différentes pratiques des services de renseignement américains mais aussi d'autres pays, notamment le Royaume-Uni et la France. Les nombreux faits publiés par la presse à partir de cette source ne peuvent être tous considérés comme établis. Toutefois, peu d'entre eux ont été démentis par les autorités des États concernés, et quelques uns ont été officiellement confirmés, notamment par la levée du secret défense sur certains documents. En outre, plusieurs rapports et avis ont été adoptés par des organismes publics, notamment la commission convoquée par le président des États-Unis pour proposer une réforme du cadre juridique du renseignement[326], le Parlement européen[327] et le G29[328]. Des procédures judiciaires sont en cours devant les juridictions américaines, britanniques et françaises[329], ainsi que devant la CEDH. Ce qu'il est convenu d'appeler « *l'affaire Prism* », bien que le programme Prism ne soit que l'un de ceux révélés depuis juin 2013, est aujourd'hui un élément central du débat public sur la surveillance des communications électroniques et plus largement sur la protection des données personnelles.

326. *Liberty and Security in a Changing World*, Report and Recommendations of The President's Review Group on Intelligence and Communications Technologies, décembre 2013.

327. Résolution du Parlement européen du 12 mars 2014 sur le programme de surveillance de la NSA, les organismes de surveillance dans divers États membres et les incidences sur les droits fondamentaux des citoyens européens et sur la coopération transatlantique en matière de justice et d'affaires intérieures, n° 2013/2188(INI) ; cf. aussi « The US surveillance programmes and their impact on EU citizens' fundamental rights », note rédigée par M. Caspar Bowden pour la commission LIBE du Parlement européen, PE 474.405.

328. Article 29 Data Protection Working Party, *Opinion 04/2014 on surveillance of electronic communications for intelligence and national security purposes*, avril 2014, WP 215.

329. La Fédération internationale des ligues de droits de l'homme (FIDH) et la Ligue française pour la défense des droits de l'homme et du citoyen (LDH) ont porté plainte contre X en juillet 2013, notamment pour collecte frauduleuse de données à caractère personnel ; le parquet de Paris a ouvert une enquête préliminaire.

Le cadre de la surveillance des communications aux États-Unis et les programmes révélés par Edward Snowden

1. Le cadre juridique de la surveillance des communications aux États-Unis

La base constitutionnelle de la protection de la vie privée aux États-Unis est le quatrième amendement[330]. Dans son arrêt *Katz v. United States*[331] de 1967, la Cour suprême a jugé que le 4e amendement s'opposait à ce que des écoutes téléphoniques soient pratiquées sans un mandat délivré par un juge. Cependant, la protection du 4e amendement ne s'étend pas aux personnes non-Américaines ne résidant pas aux États-Unis[332], ni aux informations que les personnes concernées ont confié à des « tierces parties », telles que des banques ou des compagnies de téléphones ; selon une jurisprudence aujourd'hui contestée, la Cour suprême considère que les personnes qui ont confié délibérément des informations à ces tierces parties n'ont pas d'attente raisonnable de protection de leur vie privée[333].

À la suite de la révélation de pratiques étendues d'écoutes de militants des droits civiques et d'opposants à la guerre du Vietnam, des propositions de réforme ont été présentées par une commission du Sénat présidée par Frank Church, donnant lieu à l'adoption du *Foreign Intelligence Surveillance Act* (FISA) de 1978.

Le FISA n'habilite le gouvernement à intercepter les communications sur le sol des États-Unis dans le but d'obtenir des renseignements sur les agissements de puissances étrangères ou de groupes terroristes que sur autorisation préalable d'une juridiction spécialisée, la *Foreign Intelligence Surveillance Court* (FISC)[334]. La FISC est composée de juges fédéraux nommés par le président de la Cour suprême. La FISC ne doit délivrer de mandat que si le gouvernement démontre qu'il est probable (« *probable cause* ») que la personne ciblée soit engagée dans de tels agissements.

En réponse aux attentats du 11 septembre 2001, les pouvoirs d'interception des communications ont été étendus par des décisions du Congrès et du Président. *Le Patriot Act* du 26 octobre 2001 a créé au sein du FISA une « section 215 », qui permet à la FISC d'ordonner à toute entité de communiquer au gouvernement tout document ou objet, dès lors qu'il existe des bases raisonnables pour penser que ces documents ou objets sont pertinents dans la lutte contre le terrorisme ou d'autres activités clandestines. C'est dans le cadre de la section 215 que la

330. « *Le droit des citoyens d'être garantis dans leurs personnes, domiciles, papiers et effets, contre des perquisitions et saisies déraisonnables ne sera pas violé, et aucun mandat ne sera délivré, si ce n'est pour un motif plausible, soutenu par serment ou déclaration solennelle, ni sans qu'il décrive avec précision le lieu à fouiller et les personnes ou choses à saisir* ».

331. 389 US. 347, 351 (1967).

332. *United States v. Verdugo-Urquidez*, 494 US. 259, 265-266 (1990)

333. *Miller v. United States*, 425 US 435 (1976) et *Smith v. Maryland*, 442 US 735 (1979).

334. La création d'une juridiction spécialisée est justifiée par le fait qu'elle est habilitée à connaître d'éléments couverts par le secret défense.

FISC a autorisé à partir de 2006 la collecte systématique (« *bulk connection* ») des métadonnées des opérateurs téléphoniques et leur stockage par la NSA. Dans le cadre de cette autorisation, la NSA peut consulter les métadonnées de l'ensemble des appels passés par une cible pour lesquels il existe un « soupçon raisonnable et motivé » (« r*easonable and articulate suspicion* »), celles des personnes appelées par la cible (le « deuxième saut »), et même si nécessaire celles des personnes appelées par les personnes appelées par la cible (le « troisième saut »[335]).

Les *National Security Letters* (NSL) ont été créées par le Congrès à la fin des années 1970. Elles permettent au FBI et à d'autres agences fédérales d'exiger dans le cadre de leurs investigations des documents tels que des relevés bancaires ou téléphoniques, sans autorisation judiciaire préalable. Le *Patriot Act* a facilité l'adoption des NSL, notamment en supprimant l'exigence d'une suspicion particulière et en permettant au FBI d'ordonner au destinataire de la NSL de garder le secret sur cette demande. 21 000 NSL ont été émises par le FBI en 2012.

En l'absence de protection par le 4e amendement, il a toujours été considéré que l'écoute des non-Américains à l'étranger relevait des prérogatives du Président. L'*Executive Order 12333*, émis par le président Reagan en 1981, régit ainsi la collecte de renseignements à l'étranger par les agences américaines. Toutefois, le développement d'internet a affaibli la distinction entre communications des Américains et communications à l'étranger : les communications entre deux étrangers peuvent passer par des serveurs détenus par une société américaine. C'est pourquoi le Congrès est pour la première fois intervenu en 2008, par le *FISA Amendments Act* (FAA), pour régir l'interception des communications internationales. Lorsque la cible visée est une « *US Person* » (un Américain ou un résident aux États-Unis), l'administration doit obtenir l'accord de la FISC, comme pour une communication interne aux États-Unis. En revanche, si la cible visée est une « *non-US person* », la « section 702 » du FISA autorise l'administration à procéder à l'interception sans autorisation préalable, la FISC se bornant à autoriser les catégories d'informations recherchées (informations sur des terroristes, sur des personnes impliquées dans la prolifération d'armes de destruction massive, etc.). C'est dans le cadre de la section 702 que la collecte la plus massive est effectuée : un des juges de la FISC a relevé que 250 millions de communications sur internet étaient interceptées chaque année[336]. La NSA procède en particulier par une collecte dite « *upstream* » (en amont), qui consiste à intercepter toutes les communications transitant par les câbles des principaux opérateurs assurant l'interconnexion sur internet (opérateurs dits « *backbone* »).

335. Si l'on suppose qu'une personne appelle en moyenne 100 personnes au cours de la période de cinq ans qui peut faire l'objet des investigations de la NSA, le deuxième saut permet, à partir d'une seule cible, de consulter les métadonnées de 10 000 personnes, et le troisième saut celles d'un million de personnes.

336. Opinion du juge Bates du 3 octobre 2011, citée par le rapport précité *Liberty and Security in a Changing World*.

2. Les programmes révélés par Edward Snowden

Pour certaines d'entre elles, les révélations d'Edward Snowden ne font que mettre en lumière la mise en œuvre pratique de ce cadre légal. Il a par ailleurs dévoilé des pratiques qui avaient été autorisées par la FISC sans que cette autorisation n'ait été rendue publique. Enfin, il fait état de pratiques sortant du cadre légal.

- Le programme « *Prism* » entre dans la première catégorie, puisque comme la collecte « *upstream* », il est effectué sur la base de la section 702 du FISA. À la différence de celle-ci, les données ne sont pas collectées dans les câbles par lesquels elles transitent, mais auprès des serveurs de neuf grandes sociétés américaines de services sur internet (« *downstream* » ou en aval)[337].

- Le programme de collecte des métadonnées téléphoniques a été autorisé par la FISC dans le cadre de la section 215 du FISA, mais cette autorisation n'était pas connue, même du Congrès, jusqu'à ce que le *Guardian* et le *Washington Post* rendent public un arrêt de la FISC enjoignant à l'opérateur *Verizon* de communiquer ses métadonnées.

- D'autres programmes ne correspondent en revanche à aucune des dispositions votées par le Congrès. Le programme « *Muscular* » consisterait à accéder directement aux données transitant par les réseaux de fibre optique internes à de grandes sociétés numériques, sans les en informer. Le programme « *Bullrun* » tend à permettre à la NSA de contourner les protocoles de cryptage couramment employés dans les communications numériques, notamment en influençant leur conception pour y laisser des « portes dérobées », c'est-à-dire des vulnérabilités connues d'elle seule qu'elle peut exploiter en cas de besoin.

Les débats suscités par ces révélations sont de plusieurs ordres. Un premier débat est en cours devant les juridictions américaines sur la constitutionnalité de ces programmes, en particulier de la collecte des métadonnées téléphoniques dans le cadre de la section 215. Dans une ordonnance du 16 décembre 2013 *Klayman v. Obama*[338], le juge du tribunal du district de Columbia a fait droit à la demande d'injonction des requérants tendant à stopper la collecte de métadonnées téléphoniques les concernant. Il a considéré que la collecte systématique des métadonnées sur une période de cinq ans ne pouvait être assimilée à une recherche ciblée des appels passés par une personne et qu'elle violait les attentes raisonnables de protection de la vie privée des requérants[339]. En revanche, dans

337. Selon les documents publiés par *The Guardian*, il s'agit de *Microsoft, Yahoo !, Google, Facebook, PalTalk, Skype, Youtube* et *Apple.*

338. *Klayman e.a./Obama e.a.*, 13-0851, 16 décembre 2013.

339. Il est intéressant de relever que quelques mois plus tôt, la Cour suprême avait rejeté comme irrecevables des demandes similaires au motif que la crainte des requérants de faire l'objet d'une surveillance de leurs communications n'était basée que sur des spéculations (*James R. Clapper, Jr., Director of National Intelligence, et al., Petitioners v. Amnesty International USA, et al.*, 11-1025). Le juge du tribunal du district de Columbia s'est fondé sur les révélations intervenues en juin 2013

une ordonnance du 28 décembre 2013 *ACLU v. Clapper*[340], le juge du district sud de New York a estimé qu'il n'y avait pas de violation du 4e amendement, en reprenant notamment l'argumentation du gouvernement selon laquelle l'existence de cet outil aurait permis de prévenir les attentats du 11 septembre 2001 et en relevant qu'il ne pouvait être efficace que si la collecte était systématique[341].

En Europe, le débat se focalise sur l'atteinte aux droits des Européens portée par les programmes de surveillance américains (sujet qui sera examiné plus loin (cf. *infra* 2.3) et sur l'existence en Europe de programmes similaires. En effet, le droit de plusieurs États, notamment la France, présente certaines similitudes avec le droit américain et autorise de larges possibilités d'interception des communications par le gouvernement, à des fins de protection de la sécurité nationale :

- L'article L. 34-1 du code des postes et des communications électroniques prévoit que l'ensemble des métadonnées sont conservées pendant une durée d'un an par les opérateurs de communications électroniques, en vue de répondre aux besoins de l'autorité judiciaire, de la HADOPI, de l'ANSSI ou de la lutte contre le terrorisme. La même obligation est imposée aux hébergeurs par l'article 6 de la loi pour la confiance dans l'économie numérique.

- L'article L. 34-1-1 du code des postes et des communications électroniques[342] permet aux services de renseignement d'accéder à ces données de connexion (cf. *supra* 1.3.3 pour une présentation complète de ces dispositions).

- L'article L. 241-3 du code de la sécurité intérieure sert de base aux interceptions des communications hertziennes effectuées à l'étranger par les services de renseignement, qui ne sont pas soumises au cadre juridique des interceptions effectuées sur le territoire. Il ne fixe aucune condition à ces interceptions, si ce n'est que leur finalité exclusive doit être la « *défense des intérêts nationaux* ».

- S'agissant de la cryptographie, notre droit admet que l'État se dote de capacités permettant de lever la confidentialité de messages chiffrés. L'article 230-1 du code de procédure pénale dispose que dans le cadre d'une enquête, il est possible de faire appel à toute personne qualifiée en vue « *d'effectuer les opérations techniques permettant d'obtenir la version en clair de ces informations* », y compris, si la peine encourue est supérieure à deux ans de prison, aux « *moyens de l'État soumis au secret de la défense nationale* ». L'usage de procédés de déchiffrement est donc explicitement admis dans le cadre de la police judiciaire ; il est implicitement admis que des moyens de déchiffrement existent dans le cadre de la défense nationale, leur utilisation en dehors de la procédure judiciaire ne faisant en revanche l'objet d'aucun texte.

---

et leur confirmation par le gouvernement pour conclure que les craintes des requérants n'avaient pas un caractère purement spéculatif.

340. 13-3994.

341. "*This blunt tool only works because it collects everything.*"

342. Remplacé à compter du 1er janvier 2015 par les articles L. 246-1 à L. 246-5 du code de la sécurité intérieure.

Le programme français de collecte des métadonnées sur le territoire national a donc en commun avec le programme américain le principe d'une collecte et d'une conservation de l'ensemble de ces métadonnées. Il s'en distingue cependant sur trois aspects substantiels : il est public et entièrement défini par la loi, alors que le programme américain était secret jusqu'à juin 2013 ; les données sont conservées par les opérateurs au lieu d'être stockées par l'autorité publique ; la durée de conservation est limitée à un an, contre cinq dans le programme de la NSA. S'agissant de l'interception des communications à l'étranger, le droit français, comme le droit américain, n'applique pas les mêmes règles que pour les interceptions effectuées sur le territoire national et laisse une plus grande latitude aux services de renseignement.

Les garanties entourant la surveillance des communications doivent être renforcées sans porter atteinte à l'efficacité de la prévention du crime organisé, du terrorisme et des autres atteintes à la sécurité nationale

Dans son principe, la légitimité d'une surveillance des communications électroniques par les pouvoirs publics n'est pas douteuse. Depuis son arrêt *Klass* de 1978, la Cour européenne des droits de l'homme a constamment jugé qu'un certain degré de surveillance des communications était nécessaire, dans une société démocratique, pour assurer la sécurité. Au cours des dernières années, le Gouvernement et le Parlement ont confirmé à plusieurs reprises le choix de faire de la collecte de renseignements par l'interception des communications une des priorités de la stratégie de sécurité nationale.

C'est donc sur l'étendue de la surveillance et les garanties dont il faut l'entourer que le débat doit porter. Dans ses choix en la matière, l'État doit procéder à une analyse globale : il doit mettre en balance, d'une part, la responsabilité qui lui incombe au titre de la protection de la sécurité nationale et, d'autre part, l'ensemble des risques que la surveillance peut faire courir au droit à la vie privée, à la liberté d'expression et à la confiance des citoyens, des entreprises et des associations dans l'usage des technologies numériques.

Les risques pour les libertés fondamentales ne peuvent être mésestimés. Pour les prévenir, il n'est pas possible de se fier au seul caractère démocratique de nos institutions, qui conduirait les responsables à faire preuve de retenue dans l'utilisation des informations collectées. L'histoire montre de manière répétée que même les États démocratiques sont portés à abuser de la surveillance et qu'une fois l'information acquise, la tentation d'en faire tout usage utile est grande. Une surveillance étendue des communications peut nuire non seulement au secret de la correspondance, mais aussi à d'autres secrets protégés par la loi, tels que le secret des sources des journalistes, le secret des échanges entre un avocat et son client, le secret médical, le secret des affaires ou le secret industriel. La plupart des citoyens, parce qu'ils ont confiance dans le caractère démocratique de notre État, ne se sentent pas menacés par la capacité de celui-ci d'accéder à leurs échanges quotidiens. Mais il est possible que dès aujourd'hui, des personnes qui souhaiteraient communiquer à la presse des informations sensibles s'abstiennent de le faire, par crainte d'être aisément identifiées grâce à l'interception de leurs

communications. Or, comme l'a jugé la Cour européenne des droits de l'homme, l'accès de la presse à de telles sources est une condition du bon fonctionnement d'une société démocratique, sous la réserve qu'il s'agisse d'informations non couvertes par un secret protégé par la loi.

Sur le plan économique, il est souvent avancé que les révélations sur les pratiques de la NSA pourraient nuire à la confiance dans les sociétés américaines. Deux études réalisées à l'été 2013 ont estimé que les entreprises américaines proposant des services d'informatique en nuage pourraient subir des pertes importantes de part de marché[343], et les dirigeants de plusieurs grandes compagnies du numérique ont fait connaître publiquement leur inquiétude à cet égard. Toutefois, les entreprises françaises et plus largement européennes ne peuvent espérer récupérer ces parts de marché que si leur cadre juridique présente de fortes garanties contre les pratiques dénoncées aux États-Unis.

Le renforcement des garanties doit intéresser trois types de surveillance : la conservation et l'accès aux métadonnées sur le territoire, les interceptions judiciaires du contenu des communications et la surveillance des communications à l'étranger.

• *La conservation et l'accès aux métadonnées sur le territoire*

Trois sujets appellent un réexamen : la conservation des métadonnées, en vue de leur utilisation à des fins de prévention des atteintes à la sécurité nationale ou de police judiciaire (a) ; l'encadrement de l'accès à ces données (b) ; le contrôle de l'accès aux données (c).

(a) Le système de collecte systématique des métadonnées revêt une importance déterminante dans la protection de la sécurité nationale. Le groupe de travail interministériel sur la cybercriminalité a estimé que « *l'obligation, faite aux prestataires techniques, de stockage des données durant une certaine durée est, eu égard au temps policier et judiciaire, une condition sine qua non de l'efficacité de l'action* ». Toutefois, on a vu qu'une interprétation sévère de l'arrêt *Digital Rights Ireland*, condamnant le principe même de la conservation systématique, ne pouvait être exclue.

Dans cette perspective, le Conseil d'État a examiné la faisabilité d'un système alternatif, reposant sur des injonctions de conservation adressées par l'autorité administrative ou l'autorité judiciaire aux opérateurs de communications :

- L'autorité administrative, agissant dans le cadre des finalités définies par l'article L. 241-2 du code de la sécurité intérieure, pourrait adresser aux opérateurs de communications et aux hébergeurs des injonctions de conservation des métadonnées ; ces injonctions, justifiées par une menace au regard de ces finalités, définiraient un périmètre et une durée de conservation des métadonnées

343. D. Castro, "*How Much Will PRISM Cost the US Cloud Computing Industry*", août 2013, www2.itif.org/2013-cloud-computing-costs.pdf ; Cloud Security Alliance, "CSA Survey Results: Government Access to Information", juillet 2013, https://downloads.cloudsecurityalliance.org/initiatives/surveys/nsa_prism/CSA-govt-access-survey-July-2013.pdf.

proportionnés à la menace. Lorsqu'il s'agit de sauvegarder les « *éléments essentiels du potentiel scientifique et économique de la France* », le périmètre pourrait couvrir par exemple l'ensemble des communications entrant ou sortant d'une entreprise ou d'un secteur industriel ou de recherche particulièrement sensible, dans une temporalité adaptée à la nature de la menace. Lorsque la finalité est de prévenir la reconstitution de groupements dissous, le périmètre couvrirait les communications des personnes identifiées comme ayant appartenu à ce groupement. Lorsqu'il s'agit de la sécurité de grands évènements (compétitions ou commémorations internationales par exemple), la collecte peut être générale en ce qui concerne la nature des données mais limitée à un périmètre géographique et à une période temporelle déterminée. S'agissant de finalités plus larges, telles que la lutte contre le terrorisme ou la criminalité organisée, l'autorité administrative devrait préalablement à l'injonction rassembler des éléments attestant la pertinence de la demande au regard de ces finalités : la décision de conservation des métadonnées doit être justifiée par de premiers éléments collectés par les services laissant penser que les individus inclus dans le périmètre pourraient être impliqués dans le terrorisme ou la criminalité organisée. Dans tous les cas, l'injonction ne peut être lancée que s'il y a des éléments tangibles qui la justifient.

- L'autorité judiciaire, quant à elle, devrait dans un tel système avoir la possibilité d'enjoindre aux opérateurs de conserver des métadonnées en rapport avec l'enquête à un stade précoce de la procédure : ce pouvoir pourrait être reconnu au procureur de la République dans le cadre d'une enquête préliminaire et au juge d'instruction dans le cadre d'une information judiciaire.

Un tel système répondrait assurément aux exigences de l'arrêt *Digital Rights Ireland*, même dans son interprétation stricte. Il n'imposerait en effet, pour reprendre les termes de la Cour, qu'une conservation « *portant soit sur des données afférentes à une période temporelle et/ou une zone géographique déterminée et/ou sur un cercle de personnes données susceptibles d'être mêlées d'une manière ou d'une autre à une infraction grave, soit sur des personnes qui pourraient, pour d'autres motifs, contribuer, par la conservation de leurs données, à la prévention, à la détection ou à la poursuite d'infractions graves* » (§ 59).

Toutefois, ce mécanisme de conservation sur injonction serait nettement moins efficace que la conservation systématique du point de vue de la sécurité nationale et de la recherche des auteurs d'infraction. En effet, il ne permettrait aucun accès rétrospectif aux échanges ayant eu lieu avant que l'autorité n'identifie une menace ou une infraction : son caractère opérationnel dépendrait donc de la capacité des autorités à anticiper sur l'identité des personnes dont les données de connexion pourraient être utiles, ce qui est impossible dans le cadre de la police judiciaire. S'agissant par exemple d'un crime, l'autorité judiciaire ne pourrait avoir accès aux communications antérieures à celui-ci, donnée pourtant précieuse et parfois même indispensable pour l'identification de son auteur et de ses complices, comme l'ont montré quelques récentes affaires d'attentats terroristes.

Dans le domaine de la prévention des atteintes à la sécurité nationale, les nouveaux programmes techniques reposent sur une capacité de détection des signaux faibles, incompatible avec l'idée du pré-ciblage des personnes dangereuses. C'est en effet le volume des données recueillies, leur exhaustivité et la possibilité de « retours en arrière » qui permettent d'établir des profils, de repérer des réseaux, d'anticiper sur des comportements, de détecter de nouvelles cibles et de déjouer des menaces dont les signes avant-coureurs ne peuvent être repérés qu'à partir d'une masse considérable d'informations. En outre, en diminuant les possibilités de collecte de renseignement de la France, il restreindrait sa capacité de coopération avec les services de renseignement étrangers les plus performants et la rendrait dépendante de ses partenaires pour sa sécurité.

Il est probable que la CJUE sera amenée à lever les ambiguïtés de l'arrêt *Digital Rights Ireland* à l'occasion d'un nouveau renvoi préjudiciel sur la conformité d'une législation nationale au droit de l'Union européenne tel qu'elle l'a interprété. À cette occasion, le Gouvernement français pourrait faire valoir les arguments tendant à ne pas exclure par principe la conservation systématique des métadonnées, à condition qu'elle soit entourée de strictes garanties.

Si la CJUE validait, malgré tout, l'interprétation stricte de l'arrêt *Digital Rights Ireland*, celle-ci ne pourrait être remise en cause par la voie d'un acte de droit dérivé tel qu'une directive ou un règlement, car la Cour se fonde directement sur la Charte des droits fondamentaux de l'Union européenne, qui occupe un rang supérieur dans la hiérarchie des normes. Seul un traité ratifié par l'ensemble des États membres de l'Union, qui pourrait prendre la forme d'un protocole interprétatif de la Charte[344], pourrait alors conduire à une nouvelle lecture de celle-ci. Ce protocole interprétatif pourrait valider expressément le principe de la conservation systématique des métadonnées, tout en l'entourant des garanties nécessaires en termes de limitation de la conservation et d'accès.

(b) Sur l'encadrement de l'accès aux données, la première interrogation porte sur la nature de l'autorité qui contrôle cet accès, qu'il s'agisse du contenu des communications ou des métadonnées. S'agissant de l'accès par les autorités administratives, la loi française prévoit qu'il doit être autorisé par le Premier ministre pour les interceptions du contenu des communications et par une « *personnalité qualifiée* » placée auprès du ministre de l'intérieur (puis du Premier ministre à compter du 1er janvier 2015) pour l'accès aux métadonnées. Il pourrait paraître préférable de confier cette autorisation à une autorité administrative indépendante. Dans son arrêt *Digital Rights Ireland*, la CJUE a relevé que « *surtout, l'accès aux données conservées par les autorités nationales compétentes n'est pas subordonné à un contrôle préalable effectué soit par une juridiction, soit par une entité administrative indépendante dont la décision vise à limiter l'accès aux*

344. À l'exemple du protocole sur l'article 119 du traité instituant la Communauté européenne, annexé au traité de Maastricht, que les États avaient signé pour limiter dans le temps les effets de l'arrêt *Barber* (CJCE 17/5/1990, C-262/88) qualifiant les régimes professionnels de sécurité sociale de rémunérations et les soumettant en tant que tels au principe d'égalité entre les hommes et les femmes.

données et leur utilisation à ce qui est strictement nécessaire aux fins d'atteindre l'objectif poursuivi » (§ 62). Cette mention pourrait être lue comme condamnant un dispositif qui ne subordonnerait pas l'accès aux métadonnées à une autorisation délivrée par un juge ou une AAI, comme c'est le cas du dispositif français pour les réquisitions administratives.

Toutefois, tant le Conseil d'État, dans son avis sur la loi du 10 juillet 1991, que le Conseil constitutionnel, dans sa décision n° 2005-532 DC du 19 janvier 2006, et la Cour européenne des droits de l'homme, dans plusieurs arrêts dont l'arrêt *Kennedy c. Royaume-Uni* du 18 mai 2010 (cf. *supra* 1.3.3), ont admis qu'une telle décision pouvait être prise par une autorité gouvernementale, à condition qu'un juge ou une autorité indépendante soit doté de prérogatives de contrôle suffisantes. Il ne s'agit que d'une mention parmi d'autres dans l'arrêt de la CJUE. La responsabilité de la sécurité nationale incombe en vertu de la Constitution au pouvoir exécutif ; il est nécessaire que le Premier ministre ou ses subordonnés directs conservent la possibilité, même s'ils en usent rarement, de s'écarter de la recommandation de l'AAI chargée du contrôle.

S'agissant de l'accès à des fins de police judiciaire, celui-ci est ouvert au juge d'instruction dans le cadre d'une information judiciaire ; dans le cadre des enquêtes préliminaires et de flagrance, il doit être autorisé par le juge des libertés et de la détention[345]. Ces dispositions satisfont à l'exigence d'autorisation par une « *juridiction* » énoncée par l'arrêt de la CJUE, y compris si l'on donne au terme de « *juridiction* » le sens que lui donne la jurisprudence de la Cour européenne des droits de l'homme, qui exige l'indépendance par rapport au pouvoir exécutif[346]. En revanche, le fait que les autorités judiciaires puissent accéder aux métadonnées pour tout crime ou délit, alors que la CJUE n'a reconnu l'existence d'un motif d'intérêt général pouvant justifier la conservation et l'accès aux données de connexion que dans le cadre de la lutte contre la « *criminalité grave* », soulève une difficulté. Il devrait donc être envisagé de réserver l'accès aux métadonnées pour les infractions d'une particulière gravité.

(c) La CNCIS est composée de trois membres. Elle ne compte que cinq collaborateurs, dont seulement deux assistent directement les membres dans l'exercice de leurs missions[347]. Ses moyens n'ont pas évolué depuis la loi du 10 juillet 1991, alors que son champ de compétence a été considérablement étendu par la création d'une procédure d'accès aux métadonnées. Comme l'ont relevé tant la CNCIS elle-même au fil de ses rapports annuels qu'une mission d'information récente de l'Assemblée nationale[348], ces moyens ne sont manifestement pas suffisants pour assurer un

345. Cf. les articles 60-2, 77-1-2 et 99-4 du code de procédure pénale, respectivement pour l'enquête de flagrance, l'enquête préliminaire et l'information judiciaire.

346. CEDH, 23 novembre 2010, *Moulin c. France*, n° 37104/06.

347. Les trois autres collaborateurs assurent les fonctions de secrétariat, d'officier de sécurité et de chauffeur.

348. J.-J. Urvoas et P. Verchère, Rapport d'information de la commission des lois déposé en application de l'article 145 du règlement, par la commission des lois constitutionnelles, de la législation et de l'administration générale de la République, en conclusion des travaux

contrôle effectif de la surveillance des communications. Pour les seules demandes d'accès aux métadonnées dans le cadre de la loi du 23 janvier 2006, la CNCIS est saisie de près de 600 décisions de la personnalité qualifiée chaque semaine.

Au-delà de cet aspect quantitatif, il est possible de s'interroger sur la nature de l'autorité chargée du contrôle. Trois modèles sont envisageables : le contrôle par une autorité judiciaire ; le contrôle par une émanation du Parlement ; le contrôle par une autorité administrative indépendante. Si dans notre pays, le contrôle par le juge est réservé aux interceptions judiciaires et est écarté pour les interceptions administratives pratiquées à des fins de prévention, il est appliqué à ces interceptions préventives aux États-Unis (c'est le rôle de la FISC, décrite ci-dessus) et, dans une certaine mesure, au Royaume-Uni. Les débats que connaissent les États-Unis montrent au demeurant que le contrôle ou même l'autorisation par le juge n'est pas à lui seul une garantie suffisante[349]. En France cependant, cette solution est exclue par la jurisprudence du Conseil constitutionnel, selon laquelle la réquisition et le traitement des «données de trafic», ayant pour finalité la prévention des actes de terrorisme, constituent de pures opérations de police administrative et ne peuvent en aucun cas relever de la compétence de l'autorité judiciaire[350]. Le deuxième type de contrôle existe depuis qu'une loi du 9 octobre 2007 a créé une délégation parlementaire au renseignement (DPR) ; la loi du 18 décembre 2013 a accru ses pouvoirs, en lui donnant un rôle de contrôle et non plus seulement de suivi de l'activité des services. Toutefois, la jurisprudence du Conseil constitutionnel selon laquelle le Parlement ne peut connaître d'opérations en cours[351] ne lui permet d'exercer son contrôle qu'*a posteriori ;* la DPR ne pourrait donc pas reprendre les attributions de la CNCIS, qui contrôle les interceptions durant leur réalisation. Le modèle de contrôle par une AAI, pratiqué par la France depuis 1991, doit donc être maintenu tout en étant renforcé.

La loi est aujourd'hui muette sur l'encadrement de certaines pratiques lorsqu'elles sont effectuées dans un cadre administratif : déchiffrement des communications cryptées, sonorisation, fixation d'images ou encore captation des données informatiques ; ceci contraste avec le cadre judiciaire, pour lequel toutes ces possibilités sont expressément prévues et encadrées[352]. Comme l'avait préconisé une mission d'information de l'Assemblée nationale sur le cadre juridique des services

---

d'une mission d'information sur l'évaluation du cadre juridique applicable aux services de renseignement, mai 2013.

349. Au demeurant, le contrôle par la CNCIS n'exclut pas en France la possibilité d'un recours devant le juge administratif par un requérant qui estimerait faire l'objet d'une mesure d'interception, comme l'a rappelé le Conseil constitutionnel dans sa décision n° 2005-532 DC du 19 janvier 2006 (§ 12).

350. Décision n° 2005-532 du 19 janvier 2005, *Loi relative à la lutte contre le terrorisme et portant dispositions diverses relatives à la sécurité et aux contrôles frontaliers,* cons. 5.

351. Décision n° 2001-456 DC du 27 décembre 2001, § 45, au sujet de la commission de vérification des fonds spéciaux.

352. Respectivement par les articles 230-1, 706-96 et 706-102-1 du code de procédure pénale.

de renseignement[353], les investigations menées par les services de renseignement pourraient être autorisées par les textes normatifs, et ainsi sécurisées, notamment au regard de l'exigence de prévisibilité de la loi de la CEDH, tout en étant assorties des garanties nécessaires.

Enfin, se pose la question délicate de la capacité à appréhender et à contrôler des pratiques, voire des programmes de renseignement qui sortiraient du cadre légal. Comme le relève l'avis précité du G29 du 10 avril 2014, les révélations récentes ont montré que ce risque ne pouvait être négligé. Ainsi, les mécanismes sophistiqués de *reporting* prévus par le système britannique n'avaient jamais fait état du programme « *Tempora* » d'interception des câbles transatlantiques. Pour parer à un tel risque, l'instauration de procédures de signalement, permettant à des agents des services de renseignement de saisir l'AAI chargée du contrôle ou la DPR d'informations sur des pratiques illicites, dans un cadre préservant le secret de la défense nationale, devrait être envisagée.

• *Les interceptions judiciaires du contenu des communications*

Par nature, les interceptions judiciaires du contenu des communications ne soulèvent pas les mêmes difficultés que la conservation générale des métadonnées. En premier lieu, elles sont décidées par l'autorité judiciaire. En deuxième lieu, elles sont par nature ciblées, puisqu'elles s'inscrivent dans le cadre d'une enquête ayant pour objet d'appréhender les auteurs d'une infraction. En troisième lieu, les résultats de ces investigations ne peuvent donner lieu à une condamnation qu'après avoir été versés au dossier de la procédure pénale et, de ce fait, être soumis au principe du contradictoire.

En outre, le cadre issu de la loi du 10 juillet 1991, qui n'a que très peu été modifié depuis, comporte plusieurs garanties supplémentaires :

- une interception ne peut être décidée que si la peine encourue est d'au moins deux ans d'emprisonnement ;

- elle doit être décidée par un magistrat indépendant, soit le juge d'instruction lorsqu'une information judiciaire est ouverte, soit le juge des libertés et de la détention dans le cadre d'une enquête préliminaire ;

- seule la correspondance utile à la manifestation de la vérité est retranscrite ;

- les avocats, les journalistes et les parlementaires bénéficient de protections spéciales : les correspondances avec un avocat relevant de l'exercice des droits de la défense ou avec un journaliste qui méconnaîtraient le secret des sources ne peuvent être retranscrites ; le bâtonnier ou le président de l'assemblée doivent être informés.

Il n'apparaît pas nécessaire de prévoir de nouvelles garanties, le système actuel assurant un équilibre satisfaisant entre l'exigence d'efficacité des enquêtes et la protection du droit à la vie privée.

---

353. J.-J. Urvoas et P. Verchère, *Mission d'information sur l'évaluation du cadre juridique applicable aux services de renseignement*, Assemblée nationale, mai 2013.

• *La surveillance des communications à l'étranger*

Le cadre législatif français ne s'applique pas à l'ensemble des communications électroniques. Le code de la sécurité intérieure ne définit pas son champ d'application et la jurisprudence n'a pas eu l'occasion de trancher cette question. Mais il s'agit nécessairement du champ de la loi française relative aux opérateurs de communications électroniques : en effet, les mesures d'interceptions ou d'accès aux métadonnées ne peuvent s'appliquer que si l'opérateur est soumis pour les communications concernées à la loi française, qui régit notamment la conservation des données et le droit d'accès des autorités. Dès lors que l'une des deux parties à une communication relève de ce champ, les garanties prévues par le code de la sécurité intérieure s'appliquent. En revanche, si les deux parties sont en dehors de ce champ, ces garanties ne s'appliquent pas. Seul s'applique alors l'article L. 241-3 du code de la sécurité intérieure, anciennement article 20 de la loi du 10 juillet 1991, qui permet aux pouvoirs publics de prendre des mesures « *pour assurer, aux seules fins de défense des intérêts nationaux, la surveillance et le contrôle des transmissions empruntant la voie hertzienne* », sans que s'applique le cadre législatif des interceptions administratives et judiciaires.

Le fait que les garanties entourant l'interception des communications soient moindres lorsqu'elles se situent à l'étranger plutôt que sur le territoire se justifie, bien qu'il fasse aujourd'hui l'objet de controverses. La différenciation de même nature (même si elle se fonde davantage sur la nationalité des personnes concernées) à laquelle procède la législation américaine a été l'un des points les plus critiqués à la suite des révélations de l'affaire *Prism*, même si cet aspect n'était en rien secret ; elle fait en particulier l'objet d'une dénonciation virulente du Parlement européen dans sa résolution du 12 mars 2014. Pourtant, dès lors que les personnes situées à l'étranger échappent à la juridiction de l'État, l'interception de leurs communications n'est pas susceptible de porter atteinte à leurs droits dans la même mesure que si elles se situaient sur le territoire ; elles ne peuvent en particulier faire l'objet de mesures juridiques contraignantes qui se fonderaient sur les éléments collectés. Dans une affaire *Liberty et autres c. Royaume-Uni*[354], qui mettait en cause la législation britannique relative aux interceptions à l'étranger, distincte des interceptions effectuées sur le territoire, la CEDH n'a pas remis en cause le principe de cette différenciation. Comme il sera exposé plus loin, le droit international public ne condamne pas non plus les activités conduites par un État de collecte de renseignements à l'étranger (cf. *infra* 2.3.2).

Pour autant, certaines garanties doivent entourer l'interception des communications à l'étranger. Le droit à la vie privée est garanti par la convention européenne de sauvegarde des droits de l'homme et le pacte international relatif aux droits civils et politiques à tous les individus. Dans l'arrêt *Liberty et autres c. Royaume-Uni*, la CEDH a jugé que la législation britannique ne satisfaisait pas à l'exigence de prévisibilité de la loi, rappelant sa jurisprudence constante selon laquelle « *la loi doit user de termes assez clairs pour indiquer à tous de manière suffisante en quelles circonstances et sous quelles conditions elle habilite la puissance publique à prendre pareilles mesures secrètes* ». Le même raisonnement pourrait s'appliquer à l'article L. 241-3, compte tenu de sa rédaction particulièrement allusive.

354. CEDH 1er juillet 2008, n° 58243/00.

2.2. Promouvoir les libertés à l'ère des « plateformes »

Le bilan du numérique, entre opportunités et risques, ne se présente pas de la même manière pour la protection de la vie privée et des données personnelles, d'une part, et pour la liberté d'expression, la liberté d'association et la liberté d'entreprendre, d'autre part. Pour le premier groupe de droits fondamentaux, les risques l'emportent sur les opportunités du numérique, comme la capacité à nouer des relations avec les autres personnes et à choisir les aspects de sa vie privée que l'on souhaite partager. Pour le second groupe, le bilan opportunités/risques est au contraire positif : le numérique, notamment grâce à internet, favorise l'exercice de ces trois libertés.

Pour autant, le numérique, parce qu'il est un espace de libertés, favorise aussi les comportements illicites et les collaborations malveillantes. « *La liberté consiste à pouvoir faire tout ce qui ne nuit pas à autrui* », proclame l'article 4 de la Déclaration des droits de l'homme et du citoyen : lorsque les abus[355] de la liberté d'expression se développent sur internet, avec la visibilité et la capacité de diffusion que peut leur donner le réseau, les libertés sont doublement menacées, d'une part parce que cette expression porte préjudice à certaines catégories (par exemple les mineurs ou les groupes qui sont la cible de propos d'incitation à la haine), d'autre part parce que la volonté de lutter contre ces abus peut conduire les acteurs publics et privés à des réactions excessives, nuisant à la liberté de tous.

Par ailleurs, le numérique n'est pas un espace d'égalité, contrairement à ce que pouvaient espérer ses pionniers. Certains acteurs y ont acquis en l'espace de quelques années une puissance considérable. Les rapports de force peuvent être à l'origine d'une moindre liberté pour les acteurs moins puissants. Cela est d'autant plus le cas que le numérique est, plus qu'on ne le croit, un espace où certaines ressources peuvent être rares : si la bande passante du réseau progresse, les besoins de son utilisation aussi ; si toute entreprise ou tout particulier peut mettre en ligne des contenus, la véritable visibilité dépend en grande partie de classements effectués par certains sites jouant un rôle de prescripteur. Ces enjeux d'inégalité de puissance et d'allocation de ressources rares peuvent appeler, comme dans d'autres domaines de la vie économique et sociale, l'intervention des pouvoirs publics pour promouvoir la plus grande liberté possible pour chacun.

De manière significative, on retrouve dans tous les débats relatifs à l'exercice des libertés sur les réseaux numériques le rôle particulier joué par certains acteurs, que l'on peut qualifier de « plateformes ». Ce terme[356] est polysémique : une première acception couvrirait notamment les « écosystèmes d'applications »[357],

355. On emploie ici le terme « abus » dans son sens fort, celui que lui donne l'article 11 de la Déclaration des droits de l'homme et du citoyen : il s'agit des propos interdits et sanctionnés par la loi.

356. Dont l'usage a notamment été promu par l'ouvrage de Nicolas Colin et Henri Verdier, *L'âge de la multitude*, *Entreprendre et gouverner après la révolution numérique*, Armand Colin, 2012.

357. L'écosystème d'applications recouvre à la fois le support sur lequel les applications peuvent être fournies (par exemple les systèmes d'exploitation pour téléphone mobile iOS

les sites de partage de contenus[358] et les places de marché[359], bref tous les sites qui permettent à des tiers de proposer des contenus, des services ou des biens ; une seconde acception, plus large, qui est celle retenue par le rapport du Conseil national du numérique sur la neutralité des plateformes[360], couvrirait également tous les sites qui servent de point de passage pour accéder à d'autres contenus, notamment les moteurs de recherche, les agrégateurs ou les comparateurs de prix. Tous ces sites ont en commun d'être des portes d'entrée, soit pour l'expression des internautes, soit pour l'accès des internautes à d'autres biens et services, soit les deux. Selon les termes du Conseil national du numérique, les plateformes « *organisent la mise en relation entre offre et demande* », « *proposent des espaces numériques d'intermédiation qui s'accompagnent de fonctionnalités de grande valeur* » et offrent « *un support aux différentes formes d'interactions sociales entre les individus* ». Ce rôle d'intermédiation confère aux plateformes un pouvoir, à la fois économique et de prescription. Le pouvoir de prescription sur l'expression des internautes se manifeste notamment par la définition de « polices de contenus » (en anglais : « *policies* ») relatives aux contenus pouvant être mis en ligne sur la plateforme. Quant au pouvoir de prescription sur l'accès aux biens et services, il s'exerce souvent par l'application d'un algorithme classant les services tiers ou les proposant de manière personnalisée à l'internaute dont la plateforme connaît les données personnelles. Le rôle joué par les plateformes et les instruments qu'elles mettent en œuvre ont une forte incidence sur l'exercice par les tiers de leurs libertés et posent aux pouvoirs publics des questions inédites.

Le fait de mettre en avant le rôle joué par les plateformes n'implique pas une dénonciation univoque de celui-ci : les plateformes ont une utilité manifeste tant pour les internautes que pour les offreurs de biens et de services. Il s'agit seulement de constater que ce rôle leur confère un pouvoir et que le pouvoir ne peut aller sans responsabilités, sauf à déséquilibrer l'exercice des libertés. Force est aussi de constater que nombre de ces plateformes sont établies en dehors de l'Union européenne : les questions relatives à la prise en compte de leur rôle sont donc étroitement liées à celles ayant trait à la territorialité des règles de droit, traitées plus loin (cf. 2.3).

On procédera d'abord à l'examen des principes qui doivent régir les deux catégories d'acteurs privés jouant le rôle le plus important dans l'exercice des libertés sur internet : les opérateurs de communications électroniques, qui doivent respecter un principe de neutralité, et les plateformes, pour lesquelles une nouvelle catégorie

---

d'*Apple* et *Android* de *Google* ou le réseau social *Facebook*), l'interface de programmation (souvent qualifiée « d'API », pour « *Application Programming Interface* ») mise à disposition des tiers pour qu'ils développent leurs applications et le « magasin d'applications » (*AppStore* pour *Apple* et *Google Play* pour *Google*), par lequel les utilisateurs du support pourront accéder à celles-ci.

358. Comme *Youtube*, *Dailymotion*, *Instagram* ou encore les réseaux sociaux.

359. Comme *Amazon*, *eBay* ou *Leboncoin* pour la vente de marchandises ou *AirBnB* pour la location d'appartements.

360. Conseil national du numérique, *Neutralité des plateformes. Réunir les conditions d'un environnement numérique ouvert et soutenable*, mai 2014.

juridique doit être créée et qui doivent être soumises à un principe de loyauté (2.2.1). On traitera ensuite du rôle respectif des pouvoirs publics et des plateformes dans la lutte contre les contenus illicites, constitutifs d'abus de la liberté d'expression (2.2.2). On examinera dans quelle mesure une régulation des contenus audiovisuels licites peut être opérée sur internet (2.2.3). Enfin, on s'intéressera aux algorithmes, dont le rôle dans le fonctionnement des plateformes et plus largement des services numériques est central, ainsi qu'à l'encadrement de leur utilisation (2.2.4).

2.2.1. Neutralité des opérateurs de communications électroniques, loyauté des plateformes

Les opérateurs de communications électroniques et les plateformes jouent un rôle central dans l'exercice des libertés sur internet, les premiers en acheminant les communications, les seconds en proposant des services de tri aux utilisateurs dans la multitude des contenus, biens ou services accessibles. Ce rôle n'est toutefois pas de même nature : si les opérateurs de communications doivent respecter un principe de neutralité, les plateformes, que l'étude propose de ranger dans une nouvelle catégorie juridique, doivent être soumises à un principe de loyauté.

Si le principe de neutralité du net *doit être juridiquement consacré, les approches prématurément contraignantes comportent des risques*

En dépit de sa prodigieuse expansion, internet reste défini par des choix d'architecture faits au cours de ses premières années (cf. *supra* 1.1.1), notamment son caractère ouvert permettant à tout réseau local de s'y connecter, l'acheminement selon le principe du « meilleur effort », sans qualité garantie, l'absence de contrôle centralisé ou encore la dissociation de la couche des infrastructures et de la couche des usages, les routeurs acheminant les paquets de données indépendamment de leur contenu. Ces choix relevaient au départ de considérations techniques et ne faisaient pas l'objet d'une conceptualisation sur le plan des principes, et encore moins d'une traduction juridique.

C'est en réponse à des évolutions menaçant de s'écarter de ces choix d'architecture que le principe de neutralité du *net* a été défini. L'article de 2003 de Tim Wu (cf. *supra* 1.2.2) réagissait au développement aux États-Unis de pratiques de discrimination des fournisseurs d'accès à l'égard de certains services. La neutralité du *net* était un élément de l'architecture qui paraissait aller de soi ; elle est devenue un principe à préserver.

Pour déterminer si le principe de neutralité doit être consacré et protégé par la loi, il faut répondre à deux questions préalables : ce principe est-il une garantie pour des libertés fondamentales ? Est-il aujourd'hui menacé de ne plus être respecté en l'absence d'une contrainte juridique ? Il est proposé de répondre positivement à ces deux questions. Parce qu'il permet à toute entreprise, toute association ou tout particulier de bénéficier d'un égal accès à tous les internautes, le principe de neutralité est une garantie pour la liberté d'entreprendre, la liberté d'association

et la liberté d'expression. Les menaces qui pèsent aujourd'hui sur le respect de ce principe sont par ailleurs plus consistantes qu'aux débuts d'internet : la puissance de marché de certains fournisseurs de contenus est suffisamment importante et la part du trafic représentée par quelques grands sites de diffusion de vidéos assez élevée pour que le scénario d'un accaparement de la bande passante, au détriment de la masse des autres usages d'internet, soit désormais crédible. La consécration de la neutralité du *net* par la loi, déjà décidée par les Pays-Bas, la Slovénie et le Brésil dans sa « *Marco Civil da internet* » adoptée en avril 2014, doit donc être soutenue. Elle est prévue par la proposition de règlement de l'Union européenne dite « *quatrième paquet télécoms* », votée par le Parlement européen en première lecture le 3 avril 2014[361]. L'article 2 du texte voté par le Parlement définit la neutralité de l'internet comme « *le principe selon lequel l'ensemble du trafic internet est traité de façon égale, sans discrimination, limitation ni interférence, indépendamment de l'expéditeur, du destinataire, du type, du contenu, de l'appareil, du service ou de l'application* ».

Des questions se posent cependant sur l'étendue de la marge de manœuvre à laisser aux fournisseurs d'accès à internet pour déroger à ce principe. Le premier sujet concerne la possibilité de pratiquer les mesures techniques de « *gestion de trafic* ». La proposition de règlement européen est à cet égard assez voisine des recommandations formulées par l'ARCEP en 2010, en prévoyant que ces mesures doivent être « *transparentes, non discriminatoires, proportionnées et nécessaires* » pour atteindre les finalités que sont l'exécution d'une décision de justice, la préservation de l'intégrité du réseau et la prévention ou l'atténuation des effets de sa congestion (article 23.5). Le texte voté par le Parlement européen est toutefois plus restrictif que la proposition de la Commission[362].

Le débat le plus délicat est d'ordre économique et concerne la possibilité pour les fournisseurs d'accès de passer des contrats avec des fournisseurs de contenus relatifs à des « services spécialisés » (parfois appelés « services gérés »), pour lesquels ils garantiraient une qualité de services supérieure à celle de l'internet en « meilleur effort ». Tous admettent la nécessité de permettre l'existence de ces services gérés, tels que ceux fournis depuis les années 2000 dans les offres dites « *triple play* » de téléphonie et de télévision, et qui peuvent concerner aussi la télémédecine, le vote en ligne ou d'autres usages innovants, est admise par tous, mais leur définition ne recueille pas de consensus. Le texte initial de la Commission a été jugé trop libéral par une majorité de parlementaires européens. La définition votée le 3 avril 2014 est

361. Dans le cadre de la procédure législative ordinaire (anciennement dénommée « *codécision* »), le texte doit encore faire l'objet d'une position commune du Conseil, puis d'un accord entre le Parlement européen et celui-ci.

362. Il supprime la possibilité de mesures de gestion du trafic destinées à prévenir les communications non sollicitées et exige que la congestion du trafic soit « *temporaire et exceptionnelle* », alors que la proposition de la Commission parlait de congestion « *temporaire ou exceptionnelle* ».

critiquée, notamment par les opérateurs de télécommunications, comme étant cette fois trop restrictive et risquant de faire obstacle à l'innovation[363] ; le Gouvernement français s'y était également opposé pour ce motif.

Les craintes formulées par une majorité de parlementaires européens et par de nombreuses ONG contre la rédaction proposée par la Commission peuvent être comprises, car elle revêtait un caractère quelque peu tautologique : tout service faisant l'objet d'un accord tendant à garantir sa qualité était qualifié de service spécialisé. Dès lors, cette possibilité aurait pu être largement utilisée, jusqu'à nuire à la qualité générale d'internet. À l'inverse, la rédaction adoptée par le Parlement européen fait obstacle au développement de certains usages utiles qui ne correspondraient pas à la définition très stricte qu'il a adoptée. Il ne faut pas non plus empêcher les opérateurs de télécommunications d'obtenir un financement complémentaire de la part des fournisseurs de contenus, de nature à soutenir leurs investissements dans le très haut débit. Le risque de dégradation de la qualité générale d'internet n'étant jusqu'à aujourd'hui pas avéré, l'approche adoptée par l'ARCEP depuis 2010, s'appuyant sur le droit souple et consistant à développer la mesure de la qualité d'internet afin de détecter toute tendance à la dégradation, était plus pertinente. L'approche du Parlement européen apparaît en revanche prématurément contraignante. Une voie consistant à revenir à une définition plus souple des services spécialisés, tout en prévoyant des garanties plus fermes en cas de dégradation de la qualité générale d'internet, pourrait donc être envisagée ; ses modalités seront exposées plus loin (cf. 3.1.2).

La nécessaire définition d'une nouvelle catégorie juridique pour les plateformes

L'article 6 de la LCEN organise une *summa divisio* entre les intermédiaires techniques, dont la responsabilité civile et pénale est limitée, et les éditeurs de site, dont le régime de responsabilité est analogue à celui des éditeurs de la presse écrite (cf. l'encadré ci-dessous pour un rappel des définitions). Cette distinction se fonde sur l'idée que les intermédiaires tels que les hébergeurs ont un rôle purement passif qui ne leur donne pas connaissance des informations qu'ils stockent. L'évolution de la technique et des usages numériques conduit cependant à s'interroger sur la qualification de certains sites. En effet, nombre de plateformes ne se contentent pas de stocker passivement les offres des sociétés tierces ou les contenus mis en ligne, elles les organisent en les indexant et en faisant le cas échéant des recommandations personnalisées aux internautes. Dans un arrêt *L'Oréal c/ e-Bay*, la Cour de justice de l'Union européenne a jugé que le statut

363. Le Parlement européen a ajouté deux restrictions : d'une part, alors que la proposition de la Commission qualifiait de services spécialisés tout service faisant l'objet d'un accord garantissant une qualité supérieure à celle d'internet, le Parlement européen a précisé que cette qualité supérieure devait être nécessitée par la fonctionnalité du service (article 2) ; d'autre part, alors que la proposition de la Commission demandait seulement que la fourniture des services spécialisés « *ne porte pas atteinte d'une manière récurrente ou continue à la qualité générale des services d'accès à l'internet* », le texte du Parlement exige qu'elle ne « *porte pas atteinte à la disponibilité ou à la qualité des services d'accès à l'internet* » (article 23.2).

d'hébergeur ne pouvait s'appliquer à un site de place de marché que si celui-ci ne joue pas « *un rôle actif qui lui permette d'avoir une connaissance ou un contrôle des données stockées* » et que « *ledit exploitant joue un tel rôle quand il prête une assistance laquelle consiste notamment à optimiser la présentation des offres à la vente en cause ou à promouvoir celles-ci* » (CJUE, Gde Ch., 12 juillet 2011, C-324/09). Dans une autre affaire concernant *e-Bay*, la Cour de cassation a repris le même raisonnement et confirmé l'arrêt de la cour d'appel de Paris écartant la qualification d'hébergeur (Com. 3 mai 2012, *e-Bay contre Société Parfums Christian Dior et autres*, n° 11-10.508).

Intermédiaire technique, hébergeur, éditeur : rappel des définitions légales

Les catégories dans lesquelles sont couramment rangés les principaux acteurs d'internet sont définies par la directive n° 2000/31/CE du 8 juin 2000 sur le commerce électronique, transposée en France par la LCEN. On distingue :

Les intermédiaires techniques : La qualification d'intermédiaire technique regroupe les trois catégories définies par la section 4 du chapitre II de la directive : les acteurs assurant une prestation de « *simple transport* », ceux assurant la forme de stockage dite « *caching* » et les hébergeurs. Ces trois catégories ont en commun de ne jouer qu'un rôle « *technique et passif* » dans l'acheminement des informations. Elles bénéficient d'un régime de responsabilité limitée et d'une absence d'obligation générale en matière de surveillance.

Les prestataires de « *simple transport* » : L'article 12 de la directive s'applique aux fournisseurs d'accès à internet et à ceux qui assurent l'interconnexion sans lien direct avec les utilisateurs finaux. Il est transposé en France par l'article L. 32-3-3 du code des postes et des communications électroniques.

Les prestataires de « *caching* » : L'article 13 de la directive définit le « *caching* » comme le « *stockage automatique, intermédiaire et temporaire de cette information fait dans le seul but de rendre plus efficace la transmission ultérieure de l'information à la demande d'autres destinataires du service* ». Il est transposé par l'article L. 32-3-4 du code des postes et des communications électroniques.

Les hébergeurs : L'article 14 de la directive définit l'hébergement comme le service « *consistant à stocker des informations fournies par un destinataire du service* ». Le 2. du II de l'article 6 de la LCEN, un peu plus développé, définit les hébergeurs comme « *les personnes physiques ou morales qui assurent, même à titre gratuit, pour mise à disposition du public par des services de communication au public en ligne, le stockage de signaux, d'écrits, d'images, de sons ou de messages de toute nature fournis par des destinataires de ces services* ».

Les éditeurs : La directive sur le commerce électronique ne traite pas des éditeurs, sinon en creux : ils ne font pas partie des catégories bénéficiant d'un régime de responsabilité limitée. Le III de l'article 6 de la LCEN les définit comme « *les personnes dont l'activité est d'éditer un service de communication au public en ligne* ». La qualification d'éditeur implique la maîtrise effective du contenu. Les contenus mis en ligne par l'éditeur engagent sa responsabilité civile et pénale.

La qualification juridique des moteurs de recherche et, de manière sous-jacente, leur responsabilité à l'égard des contenus éventuellement illicites auxquels ils renvoient, fait particulièrement débat. Saisie sur renvoi préjudiciel de la Cour de cassation de la qualification du service de référencement *AdWords* de *Google*[364], la CJUE a appliqué le même critère du « *rôle actif* » ; tout en laissant au juge national le soin de qualifier le service de *Google*, la CJUE a relevé que « *Google procède, à l'aide des logiciels qu'elle a développés, à un traitement des données introduites par des annonceurs et qu'il en résulte un affichage des annonces sous des conditions dont Google a la maîtrise* » et que « *Google détermine l'ordre d'affichage en fonction, notamment, de la rémunération payée par les annonceurs* » (CJUE, Gde Ch., 23 mars 2010, *Google France et Google Inc c/ Louis Vuitton Malletier*, C-236/08, § 115)[365]. Le débat judiciaire est toujours en cours : poursuivi sur le terrain de la responsabilité civile par un acteur qui estimait que *Google* était responsable d'un lien référencé par AdWords renvoyant à un article mettant en cause sa vie privée, la cour d'appel de Paris, dans un arrêt du 11 décembre 2013, a retenu la qualification d'hébergeur et annulé le jugement du TGI qui s'était prononcé en sens inverse.

S'agissant du service de recherche « *naturelle* », le tribunal de grande instance de Paris, dans un jugement du 6 novembre 2013, a écarté la qualification d'hébergeur, retenant, en se fondant sur des documents émanant d'ailleurs de la société *Google* elle-même, l'existence d'un « *choix éditorial* » quant au classement des contenus, la société ayant une entière liberté dans la détermination de son algorithme[366]. L'arrêt *Google Spain* du 13 mai 2014 de la CJUE, s'il porte sur un sujet distinct, celui de la qualification comme responsable de traitement des données personnelles, s'inscrit dans cette tendance à l'affirmation de la responsabilité des moteurs de recherche.

La *summa divisio* issue de la directive sur le commerce électronique est donc aujourd'hui sujette à de fortes incertitudes quant à la démarcation entre les deux catégories d'éditeur et d'intermédiaire technique. Il est probable que dans les prochaines années, des décisions juridictionnelles écarteront la qualification d'hébergeur pour les principales catégories de « plateformes » présentées ci-dessus : après les places de marché et les moteurs de recherche, suivront les réseaux sociaux, les plateformes de partage et les magasins d'applications. Tous ces acteurs perdront alors le régime de responsabilité limitée qui favorise leur activité. Il apparaît nécessaire de remettre en cause une distinction aujourd'hui dépassée.

Deux questions sont toutefois à distinguer. La définition des hébergeurs retenue par la directive sur le commerce électronique, reposant sur le caractère « *purement*

364. Lorsque l'internaute formule une requête sur *Google*, il reçoit d'une part les résultats de la recherche « *naturelle* », dans l'ordre défini par l'algorithme de *Google*, d'autre part les résultats des sites ayant acheté sur *AdWords* des mots-clés correspondant à sa recherche. La question de la qualification du service *AdWords* se distingue donc de celle de la qualification du service de recherche naturelle.

365. À la suite à cet arrêt de la CJUE, la Cour de cassation a cassé l'arrêt de la cour d'appel au motif qu'il n'avait pas retenu les bons critères pour écarter la qualification d'hébergeur et renvoyé l'affaire au fond devant la cour d'appel de Paris .

366. *Mosley c/ Google Inc*, n° 11/07970.

technique, automatique et passif » de leur activité (considérant 42), doit être reconsidérée. En revanche, l'idée selon laquelle la responsabilité de la plateforme à l'égard des contenus mis en ligne sur son site doit être limitée, afin d'éviter qu'elle n'exerce une censure sur leurs auteurs, conserve toute sa force. Ce n'est pas parce que les plateformes jouent aujourd'hui un rôle actif dans la présentation et la hiérarchisation des contenus qu'elles ont à leur égard une responsabilité équivalente à celle de leurs auteurs. Si des obligations de surveillance doivent leur être imposées, elles devraient être proportionnées à la gravité des infractions recherchées et au dégré de risques de censure abusive. C'est sans doute cette voie de la redéfinition de la notion d'hébergeur, tenant compte de leur rôle désormais actif mais maintenant la limitation de leur responsabilité, qu'il convient aujourd'hui d'explorer. Il sera proposé en 3.1.2 de créer une nouvelle catégorie juridique, celle des plateformes, définies comme l'ensemble des services de partage, de référencement et de classement de contenus, biens ou services édités ou fournis par des tiers.

Si le principe de neutralité n'est pas pertinent pour les plateformes, celles-ci doivent respecter le droit de la concurrence et sont tenues à la loyauté envers leurs utilisateurs

Il est parfois proposé d'étendre le principe de neutralité au-delà des seuls opérateurs de communications et de l'appliquer aux plateformes[367]. Les partisans de la neutralité des plateformes soutiennent qu'elles jouent un rôle au moins aussi important que celui des opérateurs de communications dans l'accès des internautes à de nombreux contenus et services. Parmi ces partisans, les opérateurs de communications mettent en avant le partage de la valeur qui s'opère aujourd'hui en la faveur des grandes plateformes et à leur détriment ; ils insistent sur le fait que les obligations qui seraient mises à leur charge, en vertu du principe de neutralité des réseaux, devraient être contrebalancées par un principe similaire de neutralité desdites plateformes. Cet aspect n'est pas traité par la proposition de règlement européen, qui ne concerne que les opérateurs de communications.

Les obligations des plateformes ne peuvent pourtant être envisagées dans les mêmes termes que celles des fournisseurs d'accès. L'objet de ces plateformes est de fournir un accès organisé, hiérarchisé ou personnalisé aux contenus mis à disposition sur leur site ou auxquels elles donnent accès. En vertu du principe de neutralité du *net*, un fournisseur d'accès doit traiter de la même manière tous les sites internet ; un tel traitement égalitaire ne peut être demandé à un moteur de recherche, puisque l'objet même d'un moteur de recherche est de hiérarchiser les sites internet. Les plateformes n'ont pas une responsabilité analogue à celle des gestionnaires d'infrastructures d'un réseau qui doit être universellement accessible : elles peuvent, dans le cadre de leur liberté contractuelle, exercer une sélection des services proposés. L'avis du Conseil national du numérique, s'il emploie le terme de neutralité, ne préconise pas en réalité d'imposer aux plateformes une obligation d'égal traitement analogue à celle incombant aux opérateurs de communications.

367. Cf. le rapport précité du Conseil national du numérique sur la neutralité des plateformes.

Pour autant, les plateformes sont ou devraient être soumises à plusieurs catégories d'obligations. Le droit actuel les assujettit déjà aux obligations résultant du droit de la concurrence, pour les relations des plateformes entre elles et avec les autres entreprises (a), et du droit de la consommation et du principe de loyauté dont il est porteur, pour les relations avec les internautes (b). L'utilisation qu'elles font des algorithmes justifie que leur soient imposées des obligations spécifiques que le droit actuel ne prévoit pas, ou ne prévoit que de manière incomplète ou insuffisante (cf. 2.2.4).

(a) Le droit de la concurrence permet de limiter la capacité d'une plateforme en position dominante sur son marché à en abuser, tant à l'égard de ses concurrents que des sociétés tierces qui recourent à ses services. Ainsi, l'Autorité de la concurrence, en relevant dans son avis du 14 décembre 2010 que *Google* était en position dominante sur le marché de la publicité en ligne liée aux recherches, en a déduit que cette société ne pourrait sans commettre d'abus de cette position se livrer à des pratiques telles que l'élévation de barrières artificielles à l'entrée, la conclusion d'accords d'exclusivité à la portée excessive, des prix excessifs ou des conditions d'utilisation peu transparentes pour ses clients. Engagée au niveau européen, la procédure porte sur le fait que *Google* affiche, parmi les résultats d'une recherche, ceux fournis par ses propres « *services verticaux* » (comparateur de prix, recherche d'hôtels, cartographie, agrégation d'actualités, etc.) ce qui, selon ses concurrents, nuit au développement d'une offre diversifiée dans ces secteurs. Une autre plateforme détenue par *Google*, le système d'exploitation pour smartphones *Android*, a fait l'objet d'une seconde plainte devant la Commission européenne, déposée en 2013. Il est notamment reproché à *Google* d'imposer aux constructeurs de smartphones souhaitant utiliser *Android* d'installer également des applications fournies par *Google*, telles que *Youtube* ou *Maps*. Toutes ces procédures tendent à éviter qu'une plateforme dominante ne déforme à son profit l'accès aux services et contenus disponibles sur le *net*. Elles tendent donc à garantir une certaine forme de neutralité, même si celle-ci est moins stricte que celle envisagée pour les opérateurs.

Il est parfois proposé d'aller plus loin et de considérer certaines plateformes dominantes comme des « *infrastructures essentielles* ». Dans le rapport précité *L'Union européenne, colonie du monde numérique ?,* une mission d'information du Sénat a proposé d'appliquer cette qualification à des acteurs tels que *Google* ou *Facebook*, afin de leur imposer d'assurer un accès universel à leur plateforme, dans des conditions non discriminatoires. Deux questions distinctes se posent toutefois. La notion d'infrastructure essentielle est définie de manière restrictive par la jurisprudence[368] : il faut que la ressource détenue par l'entreprise dominante soit à la fois indispensable pour l'entreprise qui offre un produit ou un service sur le marché amont, aval ou complémentaire, et impossible ou du moins considérablement difficile à reproduire dans des conditions économiques raisonnables par des concurrents seuls ou associés. Or, si le référencement par un moteur de recherche ou par un réseau social joue un rôle important dans l'exercice de nombreuses activités, il n'est pas indispensable au sens de la jurisprudence sur les facilités essentielles, car il existe en règle générale d'autres moyens pour une entreprise de se faire connaître.

368. Cf. par exemple CJCE 26 novembre 1998, *Oscar Bronner c/ Mediaprint*, C-7/97, ou Com. 12 juillet 2005, Bull. n° 163.

En revanche, l'instauration d'une régulation dite « *ex ante* », autre piste évoquée par le rapport du Sénat et qui n'est pas nécessairement liée à l'existence d'une infrastructure essentielle, pourrait être envisagée. La régulation *ex ante* de la concurrence est complémentaire de la régulation concurrentielle générale : à la différence de celle-ci, elle ne porte que sur un secteur particulier et passe par la mise en place d'un cadre réglementaire imposant des obligations *a priori* aux acteurs concernés. Selon la doctrine définie par la Commission en matière de communications électroniques, une régulation *ex ante* peut être instaurée lorsque la concurrence n'est pas effective en raison de la position dominante d'une ou plusieurs entreprises et lorsque les recours fondés sur le droit général de la concurrence ne parviennent pas à y remédier. Ces deux conditions semblent ici réunies pour certains secteurs, au vu notamment de la lenteur des procédures européennes. Reste toutefois à définir le périmètre, l'échelle géographique (nationale ou européenne) et les instruments d'une telle régulation *ex ante*, et à s'interroger sur le risque d'obsolescence rapide d'un cadre réglementaire face à l'évolution des usages numériques ; ces questions dépassent, par la finesse de l'analyse économique qu'elles requièrent, l'objet de la présente étude.

(b) Comme il a déjà été vu plus haut, les débats sur la qualification des plateformes voient souvent s'affronter deux conceptions antinomiques : l'idée de plateformes neutres, donnant accès de manière passive à un contenu préexistant sur le réseau, et celle d'acteurs disposant d'une « liberté éditoriale » leur permettant de procéder à des choix discrétionnaires. La même entreprise peut d'ailleurs se situer selon les litiges sur l'un ou l'autre terrain, l'argument de la neutralité présentant l'avantage de limiter sa responsabilité dans le cadre de la LCEN, celui de la liberté éditoriale lui évitant d'avoir à justifier ses choix de présentation. Le professeur James Grimmelmann[369] propose, au sujet des moteurs de recherche, de dépasser cette opposition en les considérant du point de vue de l'utilisateur, pour lequel ils jouent un rôle de conseiller, en proposant des sites classés selon un ordre supposé répondre à ses besoins. Si l'absence totale de biais, que réclame la théorie de l'intermédiaire neutre, n'est pas envisageable, le service de moteur de recherche supposant nécessairement des choix, la liberté n'est pas non plus aussi complète que celle des éditeurs des sites auxquels le moteur renvoie. En tant que conseiller, le moteur de recherche est tenu à une obligation de loyauté, ce qui lui interdit notamment de déformer ses résultats en raison de considérations étrangères à celles du meilleur service pour l'utilisateur, par exemple le souci de défavoriser un concurrent.

La même analyse peut sans doute être étendue à d'autres types de plateformes. Celles-ci ne sont pas tenues à une exhaustivité et une neutralité qui seraient illusoires, mais à une obligation de bonne foi, comme dans l'exécution de tout contrat, ainsi qu'aux obligations particulières d'information sur les caractéristiques du service auxquelles sont tenues les entreprises à l'égard des consommateurs non professionnels.

369. James Grimmelmann, "*Speech Engines*", University of Maryland Francis King Carey School of Law, *Legal Studies Research Paper*, No. 2014–11.

2.2.2. Définir une répartition appropriée des rôles entre administration et plateformes dans la lutte contre les contenus illicites, dans le respect des prérogatives des juges

Par contenus illicites, on entend ici tous les contenus mis en ligne qui tombent sous le coup d'une infraction prévue par la loi : il s'agit en particulier des « *crimes et délits commis par la voie de la presse ou par tout autre moyen de publication* », prévus par le chapitre IV de la loi du 29 juillet 1881 modifiée sur la liberté de la presse (notamment la provocation aux crimes et aux délits, l'apologie des crimes contre l'humanité ou du terrorisme, la provocation à la discrimination ou à la haine à l'encontre d'un groupe de personnes, la négation des crimes contre l'humanité commis durant la Seconde guerre mondiale ou reconnus comme tels par une juridiction française ou internationale, la diffamation et l'injure), des atteintes aux mineurs prévues par le code pénal (notamment la diffusion d'images à caractère pédopornographique) et de la contrefaçon. Tous ces délits, qui sont sanctionnés par des peines d'importance variable[370], ne sont pas à placer sur le même plan ; dans le commentaire de sa décision n° 2011-625 DC du 10 mars 2011 sur la LOPPSI 2, le Conseil constitutionnel a estimé que la lutte contre l'exploitation sexuelle des mineurs « *peut justifier des mesures que la préservation de la propriété intellectuelle ne peut fonder* ». Cependant, étant tous commis par la voie d'internet, ils mettent en cause les mêmes acteurs et leur prévention et leur répression soulèvent souvent des questions similaires.

Le rôle joué par les intermédiaires privés dans la lutte contre les contenus illicites fait l'objet de controverses multiples

Des controverses multiples existent aujourd'hui sur le rôle des acteurs privés dans la lutte contre les contenus illicites. Certains critiquent le caractère excessif de leur intervention, soit en raison du cadre légal, soit en raison d'initiatives unilatérales ou contractuelles des acteurs privés eux-mêmes ; d'autres estiment au contraire que leur responsabilité est définie de manière trop restrictive par la directive sur le commerce électronique.

• *Les critiques contre le caractère excessif de l'intervention des acteurs privés*

Si le principe de responsabilité limitée défini par la LCEN pour les hébergeurs est resté inchangé depuis 2004, le champ des infractions pour lesquelles ils sont tenus à certaines obligations (mise en place d'un dispositif de signalement par les internautes, information des autorités publiques[371]) a été étendu à plusieurs reprises. Il ne couvrait au départ que l'apologie des crimes contre l'humanité,

370. La diffamation ou l'injure à l'encontre d'un particulier fait l'objet d'une amende de 12 000 euros ; l'apologie de crimes contre l'humanité ou du terrorisme est punie de cinq ans d'emprisonnement et de 75 000 euros d'amende.

371. Ces obligations, spécifiques à certaines infractions et prévues par le point 7 du I de l'article 6 de la LCEN, s'ajoutent à l'obligation de retrait des contenus manifestement illicites prévue par le point 2 du I, tel qu'interprété par la décision n° 2004-496 DC du 10 juin 2004 du Conseil constitutionnel, qui est valable pour toutes les infractions.

l'incitation à la haine raciale et la pornographie enfantine ; deux lois successives ont ajouté à cette liste l'incitation à la violence, notamment aux violences faites aux femmes, et les atteintes à la dignité humaine. Un projet de loi pour l'égalité entre les femmes et les hommes, en cours de discussion au Parlement, prévoit une nouvelle extension, qui porterait sur l'incitation à la haine à l'égard de personnes à raison de leur sexe, de leur orientation ou identité sexuelle ou de leur handicap, voire sur la diffusion d'images de violence[372]. Ce texte a suscité d'importants débats, au sein et en dehors du Parlement. Ceux qui le critiquent soulignent que ce type de délits est plus difficile à apprécier pour les hébergeurs que les infractions initialement listées par l'article 6 de la LCEN, qui ont un caractère plus manifeste ; les hébergeurs pourraient donc être conduits à pratiquer trop largement le retrait et à engorger la plateforme de signalement mise en place par les pouvoirs publics. Les partisans de la disposition mettent en avant la nécessiter de lutter avec les mêmes instruments contre toutes les formes de discrimination.

Des critiques portent aussi sur le rôle joué par des acteurs privés de leur propre initiative. Le champ couvert est ici plus large que celui des hébergeurs au sens de la LCEN et englobe l'ensemble des « plateformes » définies ci-dessus (cf. supra 2.2.1). Ces plateformes définissent des « politiques » relatives aux contenus qu'elles admettent et se donnent le droit de retirer ou de ne pas afficher ceux qui n'y correspondent pas. Par exemple, *Facebook* interdit les contenus incitant à la violence, à l'automutilation ou aux troubles de l'alimentation, ainsi que l'intimidation et le harcèlement ; il « *n'accepte pas les discours incitant à la haine mais distingue cependant le sérieux de l'humour* » ; il « *impose des limites à l'affichage de certaines parties du corps* »[373]. Les conditions d'utilisation de *Google* sont exprimées de manière plus générale : « *Nous pouvons être amenés à vérifier les contenus pour s'assurer de leur conformité à la loi ou à nos conditions d'utilisation. Nous nous réservons le droit de supprimer ou de refuser d'afficher tout contenu que nous estimons raisonnablement être en violation de la loi ou de notre règlement. Le fait que nous nous réservions ce droit ne signifie pas nécessairement que nous vérifions les contenus. Dès lors, veuillez ne pas présumer que nous vérifions les contenus* »[374]. Des procédures sont mises en œuvre par ces sociétés pour examiner les contenus faisant l'objet de signalements et décider lesquels doivent être retirés[375]. L'universitaire américain Jeffrey Rosen, d'ailleurs favorable au rôle joué par ces entreprises en raison de la protection sourcilleuse de la liberté d'expression qu'elles assureraient selon lui, écrit que la personne ayant aujourd'hui le plus de

372. Ce délit est prévu par l'article 222-33-3 du code pénal, issu de la loi du 5 mars 2007 relative à la prévention de la délinquance. L'enjeu de l'ajout de ce délit à la liste prévue par l'article 6 de la LCEN serait de lutter contre la pratique dite du « *happy slapping* » (ou « *vidéolynchage* »), consistant à filmer une scène de violence pour la diffuser ensuite sur internet.

373. Mais respecte « *le droit de publier des contenus de nature personnelle, qu'il s'agisse de photos d'une sculpture telle que le David de Michel-Ange ou de photos avec un enfant au sein de sa mère* » : https://www.facebook.com/communitystandards

374. https://www.google.fr/intl/fr/policies/terms/regional.html

375. Pour une description de ces procédures, cf. J. Rosen, "The Delete Squad Google, Twitter, Facebook and the new global battle over the future of free speech", *New Republic*, 29 avril 2013, http://www.newrepublic.com/article/113045/free-speech-internet-silicon-valley-making-rules

pouvoir pour décider qui a le droit d'être entendu de par le monde n'est pas le président de la Cour suprême des États-Unis, mais la responsable de la politique des contenus chez *Google*[376], surnommée en interne « *The Decider* ».

La lutte des acteurs privés contre les contenus illicites peut également se faire dans le cadre de contrats ou d'accords informels passés entre eux. De tels accords interviennent notamment en matière de lutte contre la contrefaçon. Aux États-Unis, un accord dénommé « *Copyright Alert System* » a été conclu en 2011 entre des associations d'ayants droit et cinq grands fournisseurs d'accès pour mettre en place un système assez analogue à la loi HADOPI française, visant à détecter les internautes partageant des fichiers sur les réseaux de pair à pair en méconnaissance des droits de propriété intellectuelle, et à leur envoyer plusieurs avertissements avant que le fournisseur d'accès ne prenne des mesures à leur encontre. En France et dans d'autres pays, plusieurs grands sites de partage de vidéos proposent aux ayants droit des systèmes de reconnaissance automatique des œuvres qu'ils souhaitent voir protéger : lorsque la même œuvre est mise en ligne en méconnaissance des droits de propriété intellectuelle, le site propose aux ayants droit de retirer la vidéo ou de partager avec eux les recettes publicitaires associées à sa consultation.

Les critiques de ce rôle joué par les intermédiaires privés soutiennent que ces systèmes produisent des effets aussi contraignants que les systèmes légaux, sans légitimité démocratique et sans garantie des droits de recours. L'ONG européenne European Digital Rights (EDRi) souligne que le « *Copyright Alert System* », ainsi que d'autres accords passés avec d'autres catégories d'acteurs privés (prestataires de paiement, acteurs de la publicité), reviennent à mettre en œuvre les lois « *SOPA* » et « *PIPA* », rejetées par le Congrès américain, et le traité « *ACTA* »[377], rejeté par le Parlement européen ; ils auraient des effets comparables en termes d'automaticité du retrait des contenus en fonction des demandes des ayants droit.

• *Les critiques contre l'insuffisance du rôle joué par les acteurs privés*

Le système actuel suscite également des critiques inverses, émanant en règle générale d'autres catégories d'acteurs, ce qui illustre l'intensité des oppositions d'intérêts et des conflits de valeurs que suscite ce sujet. Il est soutenu que le cadre légal actuel ne donne qu'un rôle minimal et passif aux hébergeurs, qui doivent attendre les signalements des ayants droit.

La limitation de la responsabilité des intermédiaires techniques se fondait en partie sur la charge très lourde que ferait peser sur eux une obligation de surveillance générale. Or, les évolutions de la technique, notamment en matière de reconnaissance faciale ou de reconnaissance des contenus, rendent aujourd'hui cette surveillance beaucoup plus aisée, comme l'illustrent d'ailleurs les outils mis volontairement par les plateformes à la disposition des ayants droit. Dans son rapport sur la cybercriminalité, le groupe de travail interministériel présidé

376. Jeffrey Rosen, "The Deciders: The Future of Privacy and Free Speech in the Age of Facebook and Google", 80 *Fordham L. Rev.* 1525 (2012).

377. "*Stop Online Piracy Act*", "*Protect Intellectual Property Act*" et "*Anti-Counterfeiting Trade Agreement*".

par le procureur général Marc Robert a préconisé d'imposer aux hébergeurs une « *obligation de surveillance préventive s'agissant de la détection de contenus illicites présentant un degré de gravité particulier et se prêtant techniquement à une telle détection* »[378]. Le rapport critique la situation actuelle, qui fait peser la détection de certaines infractions sur les internautes, « *alors que les prestataires sont en mesure de le faire de manière beaucoup plus efficace* ».

Les mesures contraignantes prononcées par les juges ou les administrations suscitent également des interrogations

Les mesures contraignantes (ordre de retrait d'un contenu illicite donné à un hébergeur ou de filtrage d'un site donné à un fournisseur d'accès ou à un moteur de recherche, retraits de noms de domaine) que peuvent prendre les autorités administratives et juridictionnelles suscitent également des interrogations. L'octroi de pouvoirs contraignants à une autorité administrative est discuté en ce qui concerne tant son efficacité que sa légitimité. Le prononcé de mesures par le juge est admis dans son principe, mais il encourt les mêmes critiques que l'intervention de l'administration quant aux risques d'inefficacité et de « *surblocage* » (c'est-à-dire de blocage indirect de contenus n'ayant pas de caractère illicite) qu'il génère.

Prévu par deux lois successives, sur un champ d'infractions très large par l'article 18 de la LCEN[379] et de manière ciblée sur la pédopornographie par l'article 4 de la LOPSSI 2, le blocage sur décision administrative n'a en réalité jamais été mis en œuvre en France, les décrets d'application de ces deux textes n'ayant pas été adoptés. De fortes controverses ont animé la discussion de ces deux textes au Parlement, l'un des arguments avancés par les opposants étant que le prononcé de mesures restrictives de la liberté d'expression devrait être réservé à l'autorité judiciaire ; le Conseil constitutionnel a en effet jugé, dans sa décision n° 2009-580 DC du 10 juin 2009, qu'une autorité administrative, même indépendante, ne pouvait prendre une mesure telle que la suspension de l'accès à internet. Si le Conseil constitutionnel a admis dans sa décision n° 2011-625 DC du 10 mars 2011 sur la pédopornographie qu'une mesure de blocage d'un site avait des effets moins étendus qu'une suspension de l'accès à internet, le commentaire autorisé de la décision indique que celle-ci est justifiée par l'exigence particulière s'attachant à la protection des mineurs. L'article 18 de la LCEN a récemment été abrogé par la loi du 17 mars 2014 relative à la consommation, les travaux parlementaires faisant ressortir le souci de privilégier le recours au juge pour prononcer de telles mesures.

---

378. *Protéger les internautes. Rapport sur la cybercriminalité*, groupe de travail interministériel sur la lutte contre la cybercriminalité, juin 2014.

379. « *Dans les conditions prévues par décret en Conseil d'État, des mesures restreignant, au cas par cas, le libre exercice de leur activité par les personnes mentionnées aux articles 14 et 16 peuvent être prises par l'autorité administrative lorsqu'il est porté atteinte ou qu'il existe un risque sérieux et grave d'atteinte au maintien de l'ordre et de la sécurité publics, à la protection des mineurs, à la protection de la santé publique, à la préservation des intérêts de la défense nationale ou à la protection des personnes physiques qui sont des consommateurs ou des investisseurs autres que les investisseurs appartenant à un cercle restreint définis à l'article L. 411-2 du code monétaire et financier.* »

Moins contesté dans son principe, le prononcé de mesures contraignantes par le juge fait en revanche l'objet des mêmes doutes quant à son efficacité. Le rapport d'une mission d'information de l'Assemblée nationale sur la neutralité du *net*[380] analyse en détail les différents procédés de blocage et de filtrage (blocage d'adresses IP, de noms de domaine, d'URL ou par inspection de contenu) et conclut à une certaine facilité de les contourner. L'expérience récente de la Turquie, où le blocage de *Twitter* et de *Youtube* a été ordonné aux fournisseurs d'accès à internet avant que la justice ne le suspende, semble le confirmer, de très nombreux internautes étant quand même parvenus à y accéder. Un autre risque est celui de « *surblocage* » : la restriction d'accès frappe de manière injustifiée les pages licites d'un site bloqué ou des sites qui partagent le même nom de domaine ou la même adresse IP. Ces risques d'inefficacité et de surblocage ont été pris en compte par la CJUE dans un arrêt *UPC Telekabel* du 27 mars 2014 (C-314/12). Si la Cour admet le principe du prononcé par un juge d'une injonction de blocage d'un site diffusant des contenus contrefaisants, elle l'assortit de gardes-fous : d'une part, pour respecter la liberté d'entreprendre du fournisseur d'accès, l'injonction doit lui laisser le choix des mesures à prendre ; d'autre part, pour respecter la liberté d'expression, les mesures ne doivent pas restreindre inutilement l'accès à des contenus licites et doivent avoir une efficacité qui, sans être totale, aboutit à « *rendre difficilement réalisables les consultations non autorisées des objets protégés* ».

Encadrer le rôle joué par les acteurs privés, par la reconnaissance d'une nouvelle catégorie juridique des plateformes

La répartition des rôles entre les juges, les administrations et les acteurs privés dans la lutte contre les contenus illicites doit éviter deux écueils. Le premier serait de privilégier la répression, par l'identification des auteurs des infractions et leur traduction devant les juridictions pénales, sur la prévention par le retrait ou le blocage des contenus illicites. Cette thèse a pour elle la tradition du droit de la presse, qui écarte le contrôle *a priori* des journaux et des livres, n'admet qu'avec réticences la possibilité d'un retrait et privilégie la répression pénale *a posteriori*. Cependant, la visibilité et la rapidité de diffusion que permet internet ont pour conséquence que les infractions peuvent y entraîner des troubles beaucoup plus grands. Notre droit admet les mesures préventives : l'article 809 du code de procédure civile donne au juge des référés de très larges pouvoirs pour prévenir un dommage imminent ou faire cesser un trouble manifestement illicite ; la police administrative est toute entière justifiée par la nécessité de prévenir les troubles à l'ordre public. De manière plus spécifique, le législateur a donné au juge judiciaire de larges pouvoirs d'injonction pour faire cesser les atteintes à la vie privée, les actes de contrefaçon ou les dommages causés par les services de communication au public en ligne[381]. Ce choix n'a pas à être remis en cause. Il n'exclut bien sûr pas la punition des auteurs de ces actes ; la décision de consacrer les ressources nécessaires à cette tâche, qui n'est pas toujours aisée, relève de la politique pénale.

380. C. Erhel et L. de la Raudière, *Rapport d'information sur la neutralité de l'internet et des réseaux*, commission des affaires économiques de l'Assemblée nationale, avril 2011.

381. Respectivement aux articles 9 du code civil, 336-2 du code de la propriété intellectuelle et au 8. du I de l'article 6 de la LCEN.

Le second écueil serait de dénier aux acteurs privés le droit de décider du retrait d'un contenu, et de le réserver au juge. Une telle position n'est pas réaliste. La justice n'a pas les moyens (et ne pourrait raisonnablement les avoir) d'être saisie de tout incident relatif à la mise en ligne d'une vidéo sans accord de ses ayants droit ou à des propos discriminatoires à l'égard d'un groupe de personnes. Les inévitables délais des procédures juridictionnelles conduiraient à ce que les troubles causés par ces actes perdurent bien plus longtemps que dans la situation actuelle. Cette position n'a pas non plus, en dépit des apparences, de justification sur le plan des principes. Dès lors que certains propos ou la diffusion de certains contenus ont été interdits par la loi, les acteurs privés que sont les fournisseurs d'accès, les hébergeurs et les éditeurs ont nécessairement une responsabilité à l'égard de leur mise en ligne. Cette responsabilité peut être aménagée et limitée, mais elle doit les conduire dans certains cas à empêcher la commission d'un acte illicite.

Pour autant, les controverses sur le rôle des acteurs privés ne sont pas toutes dénuées de fondement. Un premier sujet est celui du droit de recours : lorsqu'un contenu est retiré par une plateforme, son auteur ne dispose souvent pas de voie efficace pour s'y opposer. En deuxième lieu, la définition par ces acteurs de « politiques » relatives aux contenus leur donne un pouvoir de fait sans précédent sur la définition des limites de la liberté d'expression. Le fait que les plateformes se dotent de telles politiques n'est pas critiquable en tant que tel : ce choix relève de leur liberté d'entreprendre et de leur liberté contractuelle, les conditions d'utilisation ayant le caractère d'un contrat-type proposé aux internautes, qui devient un contrat avec chacun d'entre eux lorsque ceux-ci recourent au service. Toutefois, un tel pouvoir doit être mieux encadré sur le fond et en termes de procédure. La grille de lecture définie par l'étude annuelle de 2013 du Conseil d'État, relative au droit souple, peut ici être reprise, les contrats-types étant des instruments de droit souple. Sur le fond, le droit souple ne peut conduire à méconnaître les droits fondamentaux, tels qu'ils sont conçus dans le pays où ces services sont proposés : si un contenu est illicite en vertu d'une loi nationale, une plateforme ne peut opposer le fait qu'il serait admis par sa politique ; si un contenu est licite, une plateforme ne peut le refuser pour un motif discriminatoire. Sur la procédure, l'étude sur le droit souple a conclu que pour être légitime, le droit souple devait être élaboré dans des conditions transparentes et en concertation avec les parties prenantes, ce qui n'est aujourd'hui pas le cas. Si les « *policies* » sont parfois présentées comme des règles de la communauté des utilisateurs, elles sont en réalité définies de manière unilatérale par l'entreprise. Des propositions précises sont faites plus loin sur ce sujet (cf. 3.2.2).

S'agissant enfin de l'administration, il convient d'admettre, comme en a récemment décidé le Parlement en abrogeant l'article 18 de la LCEN, que son rôle est d'avantage de recueillir les preuves des situations illicites pour en saisir le juge que de décider elle-même du retrait ou du blocage des contenus. Cependant, la décision du Conseil constitutionnel du 10 mars 2011 permet d'envisager des hypothèses limitées de prononcé de mesures contraignantes par l'administration, lorsque la nécessité de faire cesser rapidement le trouble causé par l'infraction est particulièrement impérieuse. Dans cette hypothèse, l'intervention du juge administratif, le cas échéant en référé, permet aux intéressés de disposer de voies de recours efficaces.

2.2.3. La régulation des contenus licites, notamment des contenus audiovisuels, doit reposer sur des instruments adaptés à l'environnement numérique

Dans son principe, le droit des pouvoirs publics à imposer le blocage de contenus illicites ne prête pas à discussion. Plus délicate est la question de la possibilité de promouvoir des différenciations au sein des contenus licites. Elle est étroitement liée à celle du devenir de la régulation audiovisuelle.

La régulation audiovisuelle en France est basée sur la promotion des valeurs, des principes et des objectifs énumérés par l'article 1er de la loi du 30 septembre 1986 : « *le respect de la dignité de la personne humaine, de la liberté et de la propriété d'autrui, du caractère pluraliste de l'expression des courants de pensée et d'opinion et, d'autre part, la protection de l'enfance et de l'adolescence, la sauvegarde de l'ordre public, les besoins de la défense nationale, les exigences de service public, les contraintes techniques inhérentes aux moyens de communication, ainsi que la nécessité, pour les services audiovisuels, de développer la production audiovisuelle* ». Elle est mise en œuvre par les autorisations délivrées par le CSA aux services audiovisuels diffusés par voie hertzienne et par les conventions conclues avec les services distribués par d'autres voies[382]. La migration progressive des contenus audiovisuels vers d'autres canaux, notamment les formes de diffusion « non linéaire » accessibles sur internet, oblige à faire évoluer cette régulation. La réglementation des services de médias audiovisuels à la demande (SMAD) en a été une première étape. Le fait que nombre de contenus audiovisuels n'y soient pas soumis, notamment les sites de partage de contenus mis en ligne par les utilisateurs, les sites de musique en ligne ou les SMAD ne relevant pas du champ d'application de la loi française, conduit à réfléchir à d'autres évolutions.

Deux des fondements théoriques de la régulation audiovisuelle, l'occupation du domaine public et la nécessité de réglementer des programmes « *linéaires* », ne peuvent être transposés aux services audiovisuels accessibles par internet. Le premier est tiré des règles générales de la domanialité publique qui permettent à la personne publique d'imposer des obligations d'intérêt général aux occupants et ne peuvent s'appliquer aux services audiovisuels diffusés par internet, lesquels ne passent pas par l'utilisation privative du domaine public hertzien[383]. Le second fondement tient à ce qu'il est convenu d'appeler le caractère « linéaire » des services audiovisuels classiques. Des chaînes de télévision ou de radio diffusent un programme conçu à l'avance et l'utilisateur qui accède à ces chaînes n'a d'autre choix que de les regarder

382. Notamment les chaînes diffusées sur le câble ou par ADSL et qui ne sont pas la reprise intégrale des chaînes diffusées par voie hertzienne.

383. Le fait que l'internet mobile soit diffusé par la voie hertzienne est ici sans incidence. Ce sont les opérateurs de communications, et non les éditeurs de services audiovisuels, qui sont titulaires des autorisations d'occupation du domaine public hertzien leur permettant de fournir un accès à internet. Les éditeurs de services audiovisuels, comme tous les éditeurs de services de communication au public en ligne, fournissent librement leur service sur internet, sans avoir à se soucier de la manière dont les utilisateurs y accèdent (certains y accéderont par l'internet fixe, d'autres par l'internet mobile).

dans l'ordre proposé. Sur internet, l'utilisateur peut passer comme il le souhaite d'un site à un autre et dispose donc d'une plus grande liberté de choix. La réglementation de l'audiovisuel a été en partie conçue en raison de l'influence considérable que pouvait donner à l'éditeur d'une chaîne le fait que le même contenu soit vu par des millions de personnes au même moment (ce qui justifie l'expression anglaise de « *mass media* »). Cette question de l'influence ne se présente pas dans les mêmes termes sur internet. Selon la jurisprudence constante du Conseil constitutionnel en matière de communication audiovisuelle, « *l'objectif à réaliser est que les auditeurs et les téléspectateurs, qui sont au nombre des destinataires essentiels de la liberté proclamée par l'article 11, soient à même d'exercer leur libre choix sans que ni les intérêts privés ni les pouvoirs publics puissent y substituer leurs propres décisions* »[384] ; sur internet, compte tenu de la diversité de l'offre, cette condition de libre choix peut être considérée comme étant plus aisément réalisée.

En revanche, un troisième fondement théorique est aussi pertinent sur internet que sur les moyens de communication audiovisuels classiques : celui des objectifs de valeur constitutionnelle que sont la sauvegarde de l'ordre public, le respect de la liberté d'autrui et la préservation du caractère pluraliste des courants d'expression socioculturels, ainsi que de l'intérêt général qui s'attache à la promotion de la diversité culturelle. Le droit constitutionnel et le droit international reconnaissent la possibilité d'imposer des restrictions à la liberté d'expression à condition qu'elles soient justifiées par de tels motifs et qu'elles soient proportionnées.

Le cadre juridique d'internet s'est toujours inscrit jusqu'à présent dans un modèle similaire à celui du droit de la presse, dans lequel la liberté d'expression est complète dans la limite des infractions définies par la loi, sanctionnées par le juge pénal. Ce régime diffère donc fondamentalement de la régulation audiovisuelle, qui passe par la définition d'obligations réglementaires et par des sanctions administratives. Comme il a été indiqué plus haut, les motifs d'un encadrement de la liberté d'expression par les pouvoirs publics ne sont pas aussi forts sur internet que pour les services audiovisuels classiques, et il est préférable de réserver au juge le prononcé de mesures restrictives de cette liberté.

La réglementation des contenus peut plus aisément être envisagée pour poursuivre des objectifs que la législation pénale ne permet pas d'atteindre. S'agissant de la protection des mineurs, le droit pénal est embarrassé par le fait qu'un même contenu[385] peut être vu de manière légitime par les adultes tout en risquant de porter préjudice aux mineurs qui y accéderaient. L'intervention du régulateur peut alors se justifier pour définir des obligations telles que la mise en place d'une signalétique adaptée. S'agissant de la promotion de la diversité culturelle, la voie ouverte par la directive n° 2010/13/UE relative aux services de médias audiovisuels, qui permet aux États d'imposer à ces services des obligations en matière de contribution financière à la production d'œuvres européennes ou de place consacrée aux œuvres européennes dans leur catalogue, pourrait être étendue à d'autres services

384. Cf. en dernier lieu la décision n° 2009-577 DC du 3 mars 2009, *Loi relative à la communication audiovisuelle et au nouveau service public de la télévision*, § 2.

385. Notamment les images de violence ou à caractère pornographique.

audiovisuels sur internet[386], soit comme le préconise le CSA par la voie de conventions comportant des engagements volontaires de ces services, soit par la législation, qui devrait cependant être autorisée par le droit de l'Union européenne[387].

Enfin, il faut rester prudent sur l'idée d'imposer aux intermédiaires jouant un rôle dans la distribution des services audiovisuels des obligations de différenciation entre des contenus licites. L'imposition de telles obligations aux fournisseurs d'accès à internet, par exemple par l'octroi de débits plus rapides aux sites ayant souscrit certains engagements[388], impliquerait une dérogation à la neutralité du *net*, puisque ceux-ci devraient contrôler le contenu du site sollicité par l'internaute. En revanche, la solution proposée par le CSA ne soulève pas cette difficulté, dans la mesure où elle impose des obligations de différenciation aux seuls acteurs qui distribuent des services avec lesquels ils ont établi des relations contractuelles (notamment les services gérés proposés par les fournisseurs d'accès en surplus de l'internet généraliste et les magasins d'applications des terminaux mobiles). À la différence des fournisseurs d'accès à internet, de tels acteurs ne sont pas soumis à une obligation de principe de transmettre de manière équivalente tous les contenus, qui tend à garantir la liberté d'expression. Ils procèdent à une sélection de services dans le cadre de leur liberté contractuelle ; le législateur peut dès lors intervenir pour leur imposer, dans l'exercice de cette liberté, des obligations de reprendre certains services définis en fonction de critères objectifs[389]. Toutefois, le succès de ce mécanisme de conventionnement repose sur un pari quant à son attractivité réelle pour les éditeurs de services audiovisuels numériques, attractivité qui ne pourra être vérifiée qu'à l'aune de la mise en œuvre du dispositif.

2.2.4. Prendre la mesure du rôle joué par les algorithmes et concevoir l'encadrement de leur utilisation

Prendre la mesure du rôle joué par les algorithmes et de leurs risques pour les libertés des personnes concernées

L'algorithme est au cœur du rôle d'intermédiation joué par les plateformes. Le « *PageRank* » de *Google* classe les sites *web* en fonction de leur pertinence par rapport à la requête formulée par l'internaute. Un changement de version de celui-ci peut entraîner la rétrogradation de plusieurs pages d'un site commercial

386. Notamment les sites de musique en ligne, qui sont en quelque sorte à la radio ce que les SMAD sont à la télévision, et les sites de partage de contenus audiovisuels mis en ligne par les utilisateurs.

387. En effet, la directive n° 2000/31/CE du 8 juin 2000 sur le commerce électronique ne permet pas aux États d'imposer de manière unilatérale des obligations en matière de contenu des services de la société de l'information, sauf pour des objectifs d'ordre public, de protection de la santé publique ou de la sécurité publique ou de protection des consommateurs.

388. Proposition formulée notamment par le rapport de Pierre Lescure, *Culture – acte 2. Contribution aux politiques culturelles à l'ère numérique*, mai 2013.

389. De telles obligations dites de « *must carry* » sont déjà prévues par la loi du 30 septembre 1986 pour les distributeurs de services audiovisuels par câble, satellite ou ADSL : ils doivent reprendre dans leurs « bouquets » les programmes diffusés par voie hertzienne.

et provoquer ainsi des pertes financières considérables. L'algorithme de la « *NewsFeed* » de *Facebook* détermine, parmi tous les contenus mis en ligne par les « amis » souvent très nombreux, ceux qui vont être vus par l'utilisateur ; il régit aussi le sort des annonces publicitaires. Un de ses paramètres est l'intensité récente des relations entre l'émetteur du contenu et l'utilisateur ; les vieux amis tendent donc à apparaître de moins en moins… La plateforme de réservation de VTC Uber pratique le « *surge pricing* » pour déterminer ses prix : en cas de pic de demande, elle majore ses tarifs pour augmenter le nombre de véhicules proposant leurs services, et soutient qu'elle ne fait qu'appliquer la loi du marché.

L'usage des algorithmes n'est cependant pas limité aux plateformes, et le développement du *Big Data* conduit à leur expansion dans de très nombreux domaines. Les services de ressources humaines les utilisent pour présélectionner des candidats à un emploi ou prédire le risque qu'un employé a de démissionner. Les données des passagers aériens sont traitées pour identifier des profils à risque, comme l'a illustré le débat parlementaire relatif à la mise en place du fichier dit « *PNR* » (pour « *Passenger Name Record* »), prévu par l'article 17 de la loi de programmation militaire du 18 décembre 2013[390] ; ces profils à risque feront l'objet de contrôles renforcés. Dans un tout autre contexte, mais en utilisant des méthodes similaires, certains sites de rencontre appliquent des algorithmes destinés à maximiser les chances de succès de leurs mises en relation.

L'utilité des algorithmes pour optimiser le fonctionnement d'un certain nombre de services n'est pas discutable. Ils présentent cependant trois sources de risques pour l'exercice des libertés : l'enfermement de l'internaute dans une « *personnalisation* » dont il n'est pas maître (a) ; la confiance abusive dans les résultats d'algorithmes supposés objectifs et infaillibles (b) ; l'apparition de problèmes nouveaux d'équité par l'exploitation de plus en plus fine des données personnelles (c).

(a) Bien des sites internet revendiquent la mise en œuvre d'algorithmes pour personnaliser le service rendu à leurs clients, mais ce terme est ambigu. Il peut être compris de deux manières : le service est personnalisé dans la mesure où son utilisateur peut agir pour le modifier ; le service est personnalisé dans la mesure où son exploitant traite les données personnelles de l'utilisateur pour le paramétrer. Or, la plus souvent mise en œuvre est la deuxième forme de personnalisation, dans laquelle l'internaute n'est pas acteur de son expérience, mais inscrit dans une projection que forme le site visité sur sa personnalité, ses centres d'intérêt et ses désirs. Cette projection peut plus ou moins le satisfaire selon l'efficacité de l'algorithme. Il n'en reste pas moins qu'il n'en est pas maître, ni au fait de ses mécanismes ; dans bien des cas, il n'est pas même conscient de son existence.

---

390. Le rapport de la commission des affaires étrangères et de la défense du Sénat donne les indications suivantes : « *Le « ciblage » des passagers s'appuie sur la technique de l'analyse du risque. Cette méthode est fondée sur des critères objectifs, qui, combinés entre eux, permettent de repérer en amont du départ du vol des comportements spécifiques ou atypiques de passagers. Les critères de ciblage seront prédéterminés et pourront être modifiés en fonction de l'évolution des trafics et des modes opératoires des réseaux criminels et terroristes.* ».

Poussée plus avant, la personnalisation ainsi entendue conduit à des risques d'enfermement de l'individu dans une sphère limitée de possibilités et de ségrégation des expériences de l'internet. Par construction, les algorithmes sont fondés sur la prédiction de souhaits futurs à partir d'expériences présentes et passées et ont donc un tropisme à la répétition. L'adolescent qui aime les bandes dessinées continuera à recevoir des recommandations de bandes dessinées ; il n'est pas prévu par *Amazon* qu'il puisse subitement s'intéresser à Heidegger. Les expériences proposées à des personnes différentes par un même site ne sont plus identiques : la même requête formulée sur *Google* par deux personnes différentes conduira à des résultats différents ; selon Michael Fertik, « *les riches ne voient pas le même internet que les pauvres* » et « *99 % d'entre nous vivons du mauvais côté d'un miroir sans tain* »[391]. Dans la dystopie imaginée par Pierre Bellanger, deux spectateurs de la même séance de cinéma ne peuvent plus s'en parler après, car ils n'ont pas vu la même histoire[392].

(b) Le risque de dépossession associé aux algorithmes ne concerne pas seulement les individus, il porte aussi sur les choix collectifs. En 1975, le rapport Tricot alertait déjà sur la croyance selon laquelle « *l'ordinateur ne se trompe pas* ». En 2014, il est courant de lire des présentations simplistes du *Big Data* (fort heureusement contestées), selon lesquelles il suffit de collecter beaucoup de données, de laisser travailler la puissance de calcul des machines qui va établir des corrélations, puis d'appliquer ces corrélations pour aboutir à des décisions éclairées. Les données collectées peuvent cependant être affectées de biais, les corrélations ne correspondre à aucun lien de causalité. La professeure Antoinette Rouvroy alerte à juste titre sur ce renoncement à la compréhension des causes, qui fonde pourtant la rationalité depuis l'ère moderne, et sur ce dessaisissement commode de la difficile tâche de prendre des décisions au profit d'une pseudo-objectivité machinique, qu'elle qualifie de « *gouvernementalité algorithmique* »[393].

En réalité, il y a toujours derrière les succès du *Big Data* des idées humaines, dont il faut d'ailleurs saluer l'ingéniosité, et les algorithmes sont toujours porteurs de choix ; la question est de savoir qui les comprend et les maîtrise. La complexité des algorithmes, jointe au secret industriel, conduit à une asymétrie d'information entre leurs concepteurs et ceux auxquels ils sont appliqués. En raison des progrès de « *l'apprentissage par la machine* »[394], les concepteurs eux-mêmes pourraient éprouver des difficultés à en comprendre tous les mécanismes.

---

391. M. Fertik, "*The Rich See a Different Internet Than the Poor*", *Scientific American*, vol. 308, Issue 2, 15 janvier 2013. Michael Fertik est le fondateur d'un des premiers sites « d'e-réputation ».

392. P. Bellanger, *op. cit*.

393. Cf. par exemple A. Rouvroy et T. Berns, « Gouvernementalité algorithmique et perspectives d'émancipation », *Réseaux*, 2013/1 ; voir également la contribution d'A. Rouvroy à cette étude, p. 407.

394. En anglais « *machine learning* », ces mécanismes d'apprentissage permettent aux algorithmes de s'améliorer de façon autonome en tirant les leçons des écarts entre leurs prédictions et la réalité.

(c) Tout assureur, tout banquier, tout recruteur et tout vendeur souhaiterait disposer du maximum d'informations sur son interlocuteur, afin de calculer de manière fine sa prime d'assurance, d'évaluer son risque de défaut, de jauger la qualité du candidat ou de mesurer la propension du client à accepter un prix plus ou moins élevé. Les lois actuelles encadrent la capacité de ces acteurs à acquérir des informations et à les utiliser pour différencier leurs offres. Toutefois, jusqu'à une période récente, la plus forte contrainte qui pesait sur ces acteurs ne venait pas de la loi, mais de la difficulté d'acquérir les informations[395]. La facilité de la collecte des données personnelles fait aujourd'hui disparaître cette contrainte : dans le contexte présenté au 2.2.1, il est aisé de se procurer de telles informations ou de les inférer par des algorithmes prédictifs.

Le législateur se trouve placé face au choix inédit d'accepter ou d'interdire un plus grand niveau de différenciation par l'utilisation des données, avec des conséquences importantes en termes d'équité. La difficulté de connaître la situation de chacun a longtemps créé des solidarités implicites ; est-il juste de les lever ? Certains soutiendront qu'une plus grande personnalisation est source d'équité. Ainsi, les jeunes conducteurs se voient appliquer aujourd'hui de fortes primes d'assurance, parce que les outils frustes de différenciation des risques amènent les assureurs à raisonner par classe d'âge ; l'utilisation du *Big Data* permettrait de repérer les bons conducteurs parmi les jeunes, qui verraient ainsi leur prime baisser. Toutefois, l'assurance même privée ne doit-elle pas accepter un certain degré de mutualisation entre les « *bons risques* » et les « *mauvais risques* » ? La sécurité sociale elle-même est confrontée à ce débat. Le juge des référés du Conseil d'État a récemment suspendu un arrêté modifiant les conditions de prise en charge d'un dispositif médical destiné aux personnes atteintes d'apnée du sommeil ; l'arrêté prévoyait une diminution progressive des remboursements par la sécurité sociale lorsque le patient était « *inobservant* », l'observance étant connue grâce à la transmission automatique des données d'utilisation par un capteur. Le juge des référés a considéré que le moyen selon lequel un tel choix relevait des « *principes fondamentaux de la sécurité sociale* » et donc de la compétence du législateur était de nature à créer un doute sérieux sur la légalité de l'arrêté[396].

Pour définir les principes d'une société juste, le philosophe John Rawls recourait à la fiction du « *voile d'ignorance* », situation dans laquelle chacun ignore la position qu'il occupe dans la société[397]. En reprenant cette image, on peut considérer que le droit à la protection des données personnelles a pour objet de limiter la levée du voile d'ignorance qui entoure la situation de chacun, sans pour autant l'empêcher totalement car il autorise une circulation des données bien plus grande que ce qu'elle a été dans le passé. Les implications de cette levée du voile en termes d'équité, notamment quant aux choix collectifs entre solidarité et responsabilisation plus grande grâce à la personnalisation, appellent de larges débats.

---

395. Dans *Code 2.0*, Lawrence Lessig qualifie ce type de situation de « *friction* » : le comportement des individus est régi par la loi, mais aussi et peut-être d'avantage par la friction. Lorsque la technologie fait disparaître celle-ci, le législateur est placé devant des choix inédits.

396. JRCE, 14 février 2014, *UNASSAD et autres*, n° 374699, inédit.

397. J. Rawls, *Théorie de la justice*, Seuil, 1987.

Mieux encadrer l'utilisation d'algorithmes prédictifs à l'égard des individus

Pour donner aux individus des garanties appropriées concernant les algorithmes prédictifs utilisés pour prendre des décisions à leur égard, quatre objectifs doivent être poursuivis : assurer l'effectivité de l'intervention humaine dans la prise de décision (a) ; veiller à la non-discrimination (b) ; mettre en place des garanties de procédure et de transparence (c) ; développer le contrôle des résultats produits par les algorithmes (d). Les propositions qui en résultent sont exposées ci-après (cf. *infra* 3.3.2).

(a) Le débat sur le profilage n'est pas neuf. La loi du 6 janvier 1978 prévoyait dès sa version initiale, dans son article 2[398], qu'aucune « *décision administrative ou privée impliquant une appréciation sur un comportement humain ne peut avoir pour seul fondement un traitement automatisé d'informations donnant une définition du profil ou de la personnalité de l'intéressé* ». En 1981, la CNIL a eu à connaître du projet « *GAMIN* » (pour Gestion Automatisée de Médecine INfantile), qui consistait à procéder à une exploitation systématique des certificats de santé obligatoires délivrés au cours de la grossesse et de la première année de l'enfant, dans le but d'identifier des profils d'enfants « *à risque* » devant faire l'objet d'une surveillance particulière des services de protection maternelle et infantile. La CNIL a relevé que la méthode de détermination automatique d'un profil n'était qu'un élément d'aide à la décision de classement d'un enfant comme étant à risque et qu'elle ne méconnaissait donc pas directement l'article 2. Elle a toutefois refusé d'autoriser le traitement par les motifs suivants : « *Considérant néanmoins que la finalité principale est la pré-sélection par des moyens automatisés d'enfants qui, selon la logique du système, seront ou non l'objet d'une assistance médicale et sociale ; Que le tri entre les enfants s'opère à partir d'une modélisation des facteurs de risques médico-sociaux se traduisant par la prise en compte de 170 données et par l'établissement de programmes ; Qu'une telle modélisation, même si elle permet d'obtenir le plus souvent des présomptions concordantes sur la situation des enfants, contient en elle-même des facteurs d'incertitude qui peuvent ne pas être corrigés par le contrôle ultérieur cas par cas, du médecin de P.M.I. (…) ; Qu'une confiance trop grande dans ce procédé conduirait à négliger les enfants non sélectionnés, dont certains peuvent pourtant avoir besoin d'aides particulières, et à faire reposer les priorités de soins et d'assistance sur un déterminisme contestable* »[399]. Cette délibération de la CNIL illustrait déjà la nécessité de ne pas se contenter d'une apparence d'intervention humaine. Si dans 99 % des cas, la mesure prise est celle proposée par le système automatique, alors le système présenté comme une « *aide à la décision* » est en réalité un système de décision.

398. Cette disposition figure aujourd'hui au deuxième alinéa de l'article 10, dans les termes suivants : « *Aucune (…) décision produisant des effets juridiques à l'égard d'une personne ne peut être prise sur le seul fondement d'un traitement automatisé de données destiné à définir le profil de l'intéressé ou à évaluer certains aspects de sa personnalité* ».

399. Délibération n° 81-74 du 16 juin 1981 portant décision et avis relatifs à un traitement d'informations nominatives concernant le traitement automatisé des certificats de santé dans les services de la protection maternelle et infantile.

Il convient donc de s'assurer, dans la mise en œuvre effective de la règle aujourd'hui prévue par l'article 10 de la loi du 6 janvier 1978 modifiée, que les intervenants humains dans la prise de décision disposent d'une marge de manœuvre effective. Cela peut s'évaluer *ex ante*, par la prise en compte de facteurs tels que la qualification des personnes concernées, les autres éléments à leur disposition pour prendre une décision et la présentation des processus du responsable de traitement ; cela peut aussi être contrôlé *ex post* par la mesure du pourcentage de propositions de l'algorithme qui ont été suivies. L'article 20.5 de la proposition de règlement relatif à la protection des données personnelles votée par le Parlement européen le 12 mars 2014 va dans ce sens, en disposant que « *le profilage conduisant à des mesures produisant des effets juridiques pour la personne concernée ou affectant de manière significative ses intérêts, droits ou libertés n'est pas fondé exclusivement ou principalement sur le traitement automatisé et inclut une appréciation humaine, y compris une explication de la décision prise à la suite de cette appréciation* ».

(b) La prise en compte dans un algorithme de prise de décision de facteurs tels que l'origine ethnique, la religion, l'opinion politique, l'affiliation syndicale ou l'orientation sexuelle est constitutive d'une discrimination. Quant au sexe ou à l'état de santé, ils ne peuvent être pris en compte que dans certaines hypothèses[400]. L'article 17 de la loi de programmation militaire du 18 décembre 2013 sur le fichier « *PNR* », qui sert à établir des profils de passagers à risque, prend ainsi soin de rappeler que « *sont exclues de ce traitement automatisé de données les données à caractère personnel susceptibles de révéler l'origine raciale ou ethnique d'une personne, ses convictions religieuses ou philosophiques, ses opinions politiques, son appartenance à un syndicat, ou les données qui concernent la santé ou la vie sexuelle de l'intéressé* ».

La mise en œuvre du principe de non-discrimination suscite cependant plusieurs difficultés. Tout d'abord, l'interdiction de traiter de telles données peut être contournée par l'introduction d'autres variables, en apparence anodines, qui les révèlent avec un haut degré de probabilité (par exemple, la fréquentation de tel établissement ou la lecture de telle revue, qui révélerait l'origine ou les orientations politiques ou sexuelles d'une personne). En second lieu, si les traitements de données sont déclarés voire autorisés par la CNIL, indiquant à celle-ci quelles catégories de données sont prises en compte[401], les modalités de mise en œuvre des algorithmes sont complexes et difficiles à comprendre, notamment en raison

---

400. Cf. notamment à ce sujet l'article 2 de la loi n° 2008-496 du 27 mai 2008 portant diverses dispositions d'adaptation au droit communautaire dans le domaine de la lutte contre les discriminations : le principe ne fait pas obstacle « *à ce que soient faites des différences selon le sexe lorsque la fourniture de biens et services exclusivement ou essentiellement destinés aux personnes de sexe masculin ou de sexe féminin est justifiée par un but légitime et que les moyens de parvenir à ce but sont nécessaires et appropriés* » et au calcul des primes d'assurances dans les conditions définies par le code des assurances.

401. Une autorisation préalable est notamment requise pour les traitements « *susceptibles, du fait de leur nature, de leur portée ou de leurs finalités, d'exclure des personnes du bénéfice d'un droit, d'une prestation ou d'un contrat en l'absence de toute disposition législative ou réglementaire* » (4° du I de l'article 25 de la loi du 6 janvier 1978).

du secret industriel qui les protège. C'est pourquoi le contrôle de la mise en œuvre des algorithmes, par des opérations de « *testing* », peut être une manière efficace d'appréhender les discriminations dont ils seraient porteurs. Le *Data Privacy Lab* de l'université de Harvard a ainsi mis en évidence des discriminations dans des algorithmes de publicité en ligne[402].

(c) Une personne faisant l'objet d'une décision ayant pour elle des effets significatifs et s'appuyant sur la mise en œuvre d'un algorithme prédictif devrait avoir le droit de connaître les données qui ont été utilisées, notamment pour être en mesure d'identifier les données erronées, d'obtenir une explication sur le raisonnement sous-jacent à l'algorithme et de présenter ses observations, de manière à ce que la personne humaine restant responsable de la décision puisse les prendre en compte. Selon Kate Crawford et Jason Schulz, l'application des algorithmes du *Big Data* devrait être entourée de garanties de « *due process* » analogues à celles qui régissent la procédure juridictionnelle[403].

À ce jour, l'article 10 de la loi du 6 janvier 1978 prévoit que pour les décisions prises dans le cadre de la conclusion ou de l'exécution d'un contrat, une décision n'est pas considérée comme prise sur le seul fondement d'un traitement automatisé si la personne concernée a la possibilité de présenter ses observations[404]. Le champ d'application de cette possibilité de présenter ses observations pourrait être élargi et ses conditions de mise en œuvre précisées, si besoin au moyen d'instruments de droit souple.

(d) L'asymétrie d'information associée à la mise en œuvre des algorithmes prédictifs doit être corrigée, dans l'intérêt des personnes concernées mais aussi dans celui des organisations qui les mettent en œuvre, lesquelles peuvent avoir du mal à en percevoir toutes les implications et leur accorder une confiance excessive. Les auteurs de l'ouvrage précité *Big Data. La révolution des données est en marche*, par ailleurs très favorables au développement des algorithmes prédictifs, préconisent de remédier à cette asymétrie par la création d'une profession « *d'algorithmiste* », composée d'experts en science informatique et en statistiques, soumis à une déontologie et à des contrôles analogues à ceux de professions comme les médecins ou les commissaires au compte, et qui procéderaient à des contrôles internes aux entreprises ou externes, sous la responsabilité des gouvernements, pour vérifier la validité des algorithmes.

---

402. L. Sweeney, « Discrimination in Online Ad Delivery », janvier 2013, http://dataprivacylab.org/projects/onlineads/1071-1.pdf.

403. K. Crawford et J. Schulz, "Big Data and Due Process: Toward a Framework to Redress Predictive Privacy Harms", New York University School of Law, *Public Law & Legal Theory Research Paper Series,* Working Paper n° 13-64, octobre 2013.

404. Cette disposition, introduite par la loi du 6 août 2004, a notamment permis d'autoriser les pratiques d'évaluation automatique du risque de défaut des emprunteurs (pratiques dites de « *scoring* ») : cf. la délibération n° 2008-198 du 9 juillet 2008 de la CNIL modifiant l'autorisation unique n° AU-005 relative à certains traitements de données à caractère personnel mis en œuvre par les établissements de crédit pour aider à l'évaluation et à la sélection des risques en matière d'octroi de crédit.

2.3. Rendre applicables un socle de règles impératives pour tous les acteurs du numérique, quel que soit leur lieu d'établissement

La question de la territorialité sur internet, c'est-à-dire le champ d'application des règles de droit relatives aux acteurs opérant sur internet, n'est accessible qu'à un cercle assez étroit d'initiés. Les utilisateurs d'internet ne la découvrent qu'à l'occasion d'un litige qui les confronte à la complexité des règles de conflit de lois et de juridictions du droit international privé, complexité encore accrue par le fait que l'application de leurs concepts aux réalités d'internet n'est pas aisée (cf. *supra* 1.4.2). On a vu que la jurisprudence de la Cour de justice de l'Union européenne et de la Cour de cassation en France n'a répondu que très récemment aux principales questions. Ainsi que le relevait le professeur Bénédicte Fauvarque-Causson lors d'un colloque de la Société de législation comparée sur l'informatique en nuage[405], internet a introduit le droit international privé dans la vie quotidienne des particuliers et des entreprises comme jamais auparavant.

La territorialité sur internet présente donc des enjeux de simplification et d'accessibilité du droit, mais aussi et surtout des enjeux stratégiques. Est en effet en cause la capacité des États à assurer la protection des libertés fondamentales de leurs citoyens ainsi que le droit au recours de ceux-ci. Les implications pour la concurrence entre entreprises numériques sont significatives. Le Conseil d'État propose de définir un socle de règles applicables à tous les acteurs quels que soit leur lieu d'établissement ; lorsque l'application des règles générales de conflit de lois ne conduit pas à cette solution, ces règles devraient être qualifiées de « *lois de police* » au sens du droit international privé, c'est-à-dire de règles applicables en toute hypothèse dans le champ d'application qu'elles définissent, indépendamment du jeu des règles habituelles de conflits de lois. Après avoir examiné quelles règles devraient recevoir cette qualification (2.3.1), on étudiera les questions de coopération qui se posent au sein de l'Union européenne, avec les États-Unis et avec les autres systèmes juridiques, qui conditionnent son application effective (2.3.2).

2.3.1. Définir un socle de règles impératives applicables à tous les acteurs quel que soit leur lieu d'établissement

Un nécessaire équilibre entre principe du pays de l'internaute et principe du pays du site internet

Quasiment toutes les grandes entreprises du *net* étant établies aux États-Unis, la grande masse des particuliers et des entreprises européennes se voient opposer la compétence juridictionnelle et l'application de lois de différents États américains, prévues par les conditions générales d'utilisation de ces services. Ces clauses peuvent certes être écartées dans certaines hypothèses par les juridictions

405. Allocution prononcée au colloque annuel de la Société de législation comparée, *L'informatique en nuage / le cloud computing*, le 11 octobre 2013 au Conseil d'État.

nationales, comme on l'a vu dans plusieurs affaires évoquées plus haut. Mais l'apparence est en faveur de l'application du droit américain et peut dissuader les personnes concernées d'exercer des recours pour défendre leurs droits. Pour les mêmes raisons, les sociétés américaines collectent une part prédominante des données personnelles des Européens. Une étude réalisée par trois chercheurs de l'INRIA a estimé que 87 % des dispositifs de traçage utilisés par les cent premiers sites mondiaux appartiennent à des sociétés américaines[406]. La sénatrice Catherine Morin-Desailly et Pierre Bellanger y ont vu à juste titre un enjeu de souveraineté[407].

Il serait cependant hâtif d'en déduire que les États européens ont intérêt à réclamer l'application systématique à leurs internautes de leurs règles de droit, quel que soit le pays d'origine du site internet. Il est en effet difficilement envisageable que le principe du pays de l'internaute devienne une règle générale et absolue de détermination de la loi applicable sur internet. L'essence d'internet est de permettre à tout site d'être visible dans le monde entier. Il ne peut être raisonnablement demandé à un site de se conformer à toutes les règles de droit de tous les pays du monde, ne serait-ce que parce qu'elles sont sur bien des points contradictoires entre elles, et que se conformer à certaines d'entre elles pourrait le mettre en infraction avec les règles de son propre État, auxquelles il reste en tout état de cause soumis. Un même site peut différencier certains aspects de son service en fonction de l'origine géographique de ses visiteurs, mais le coût devient prohibitif si le nombre de différenciations requises est trop important. Si les revendications des États d'appliquer leurs règles de droit à leurs internautes étaient poussées trop loin, ceci conduirait sans doute nombre de sites à renoncer à être visibles dans certains États, en rejetant les demandes de connexion des internautes dont l'adresse IP indique qu'ils résident dans les pays concernés. Il y a là un risque de « *fragmentation d'internet* », c'est-à-dire de différenciation des contenus accessibles selon les pays[408].

Une telle orientation postulerait en outre que les acteurs français ou européens seront toujours voués à être sur internet en situation de consommateurs et jamais de producteurs de services. Or, la France compte aussi des entreprises du numérique cherchant à développer leurs services à l'échelle mondiale et de leur point de vue, la sécurité juridique consiste à être régies partout dans le monde par les règles françaises. L'État doit prendre en considération les intérêts des consommateurs de services sur internet, mais aussi ceux de ses entreprises dont le développement est justement de nature à réduire le déséquilibre de puissance évoqué ci-dessus et qui menace sa souveraineté. De manière générale, la France soutient d'ailleurs de longue date le principe selon lequel les parties à un contrat

406. INRIA, C. Castelluccia, S. Grumbach et L. Olejnik, "Data Harvesting 2.0: from the Visible to the Invisible Web", The Twelfth Workshop on the Economics of Information Security, 2013.

407. Cf. le rapport et l'ouvrage précités, *L'Europe, colonie du monde numérique ?* et *La souveraineté numérique.*

408. Sur les risques de fragmentation d'internet, cf. par exemple J. F. Hill, "Internet Fragmentation. Highlighting the Major Technical, Governance and Diplomatic Challenges for U.S. Policy Makers", John F. Kennedy School of Government, University of Harvard, printemps, 2012, http://belfercenter.hks.harvard.edu/publication/22040/internetfragmentation.html?breadcrumb=%2Fpublication%2F17613%2Fgovernance_and_information_technology

peuvent choisir la loi qui leur sera applicable, principe qui figurait déjà dans la convention de Rome du 19 juin 1980. Un équilibre doit donc être recherché entre principe du pays de l'internaute et principe du pays du site internet.

La prise en compte des enjeux d'équilibre concurrentiel

Dans la recherche de cet équilibre, les distorsions de concurrence induites par les différences de cadre juridique doivent être prises en compte ; c'est la demande souvent formulée sous l'expression anglaise de « *level playing field* ». Le fait que des entreprises établies dans différents États puissent, sans aucune barrière, se concurrencer pour proposer à l'internaute des services identiques ou voisins est consubstantiel à internet. Si le principe du pays du site prévaut, alors internet est un facteur de mise en concurrence des systèmes juridiques et les entreprises dont les systèmes juridiques sont les moins protecteurs peuvent en retirer un avantage concurrentiel ; en revanche, si le principe du pays de l'internaute s'applique, alors le lieu d'établissement de l'entreprise est sans incidence.

Le sujet des règles de protection des données personnelles est ici décisif, compte tenu de l'importance de ces données dans l'économie numérique et de l'ampleur des différences entre les cadres juridiques américain et européen. Le rôle que joue cet écart de protection dans le retard européen est discuté[409]. Mais il n'est pas contestable qu'un cadre juridique européen qui ne couvrirait que les traitements de données opérés par des entreprises européennes, alors que la majeure partie des données personnelles traitées par des entreprises américaines échapperait à sa protection, n'atteindrait pas ses objectifs.

La question se pose aussi pour les obligations en matière de promotion de la diversité culturelle : l'application du principe du pays d'origine en matière de services audiovisuels au sein de l'Union européenne conduit à ce que seuls les SMAD établis en France supportent les obligations définies par le décret n° 2010-1379 du 12 novembre 2010 relatif aux services de médias audiovisuels à la demande, plus importantes que celles définies par la directive ; ce sujet a nourri les débats autour du choix du pays d'installation du site américain de vidéo à la demande Netflix pour desservir le public français.

L'analyse des distorsions de concurrence est compliquée par la fréquente superposition de problèmes de champ d'application territorial et de champ d'application matériel. C'est notamment le cas des opérateurs de communications électroniques face aux acteurs dits « *over the top* »[410], qui leur livrent une

409. Cf. p. ex. pour deux positions contrastées, C. Castelluccia et D. Le Métayer, « La vie privée, un obstacle à l'économie numérique ? », *Le Monde*, 25 août 2013, et « Pour Gilles Babinet, "il faut fermer la CNIL, c'est un ennemi de la Nation " », *L'Usine digitale*, 26 février 2013.

410. Expression qui s'explique par le fait que dans le modèle par « *couches* » qui décrit le fonctionnement d'internet, ces acteurs proposent leurs services sur la couche supérieure des contenus et des applications, alors que les opérateurs de télécommunications agissent sur la couche inférieure des infrastructures.

concurrence directe, en proposant des services substituables aux leurs[411], ou indirecte en profitant davantage de la valeur créée par les usages numériques, pour diverses raisons dont l'importance respective fait débat[412]. Les différences de cadre réglementaire sont ici doubles : d'une part, ces acteurs sont le plus souvent établis hors de l'Union européenne et appliquent leurs règles nationales dans des domaines comme la protection des données personnelles ; d'autre part, ils estiment ne pas relever de la catégorie des opérateurs de communications. *Skype* est ainsi engagé depuis plusieurs années dans un litige avec l'ARCEP, qui la considère comme un opérateur.

La définition d'un socle de règles applicables à tous les acteurs proposant des services aux internautes français ou européens, si besoin en passant par la qualification de loi de police

Le Conseil d'État préconise de promouvoir le principe du pays de destination non pour l'ensemble des règles juridiques applicables aux acteurs d'internet, mais pour un socle de règles choisies en raison de leur importance particulière dans la protection des droits fondamentaux ou de l'ordre public. Les règles du socle seraient applicables à tous les sites dirigeant leur activité vers la France ou l'Union européenne (selon que la règle est de niveau national ou européen), la notion d'activité dirigée vers un pays ayant le sens qui lui a été donné par la jurisprudence et qui a été présenté plus haut (cf. 1.4.2)[413].

Selon les sujets, trois voies peuvent être envisagées pour faire prévaloir le principe du pays de destination : l'application des règles de droit commun du droit international privé (a) ; la qualification de loi de police (b) ; la coordination des législations nationales par un traité ou un acte de droit dérivé de l'Union européenne (c).

(a) Dans certains cas, l'application des règles de droit commun du droit international privé conduit à appliquer le principe du pays de destination. Ainsi, les lois pénales définissant les limites de la liberté d'expression revêtent une grande importance pour la sauvegarde des intérêts publics et devraient faire partie du socle. L'application des règles générales sur le champ d'application de la loi pénale permet d'aboutir au résultat recherché : en effet, le responsable du site internet est responsable au titre de la loi pénale française si le site est dirigé vers le public français.

---

411. Les services de voix sur IP comme ceux de *Skype* concurrencent la téléphonie classique. Les multiples services de messagerie instantanée qui se développent aujourd'hui (*WhatsApp*, *Viber*, *Messenger*, etc.) peuvent se substituer aux SMS.

412. Parmi les facteurs avancés dans le débat public, on trouve des motifs aussi divers que l'absence de paiement des infrastructures pour accéder à l'utilisateur (sujet lié à la neutralité du *net*), la capacité supérieure à collecter et traiter des données personnelles, la relation directe et personnalisée nouée avec le consommateur ou encore la capacité supérieure à innover. Cf. à ce sujet le colloque organisé par l'ARCEP en octobre 2013, « Quelles perspectives de création et de répartition de la valeur pour les télécoms ? », http://www.arcep.fr/uploads/tx_gspublication/actes-colloque-171013-dec2013.pdf.

413. Cf. notamment CJUE, Gde Ch., 7 décembre 2010, *Pammer et Hotel Apenhof*, C-585/08.

(b) Dans d'autres cas, il est en revanche nécessaire de s'écarter de la loi désignée par les règles générales de conflits de lois. Il en va notamment ainsi lorsque sont en cause des relations contractuelles, le droit international privé permettant aux parties de choisir la loi applicable au contrat, alors que le principe du socle est de faire prévaloir la loi nationale. Il faut donc rechercher des solutions dérogeant aux règles générales de conflits de lois. Le droit international privé reconnaît à cet égard deux possibilités : l'exception d'ordre public et la loi de police[414]. L'exception d'ordre public joue *a posteriori*, après examen de la loi étrangère désignée par la règle de conflit (par exemple la loi déterminée par le contrat), dans l'hypothèse où une disposition de cette loi apparaît manifestement incompatible avec des valeurs essentielles de l'ordre juridique interne. La loi de police joue quant à elle *a priori*, avant tout examen de la règle de conflit. Il s'agit, selon les termes de l'article 9 du règlement Rome I sur la loi applicable aux obligations contractuelles, d'une « *disposition impérative dont le respect est jugé crucial par un pays pour la sauvegarde de ses intérêts publics, tels que son organisation politique, sociale ou économique, au point d'en exiger l'application à toute situation entrant dans son champ d'application* »[415]. La loi de police est plus appropriée que l'exception d'ordre public pour parvenir au résultat recherché : elle permet de faire prévaloir l'application de la règle nationale ou européenne en toute circonstance et de garantir ainsi une meilleure prévisibilité du droit applicable.

Les règles relatives à la protection des données personnelles ont vocation à entrer dans cette catégorie, dès lors qu'elles mettent en œuvre un droit garanti par la Charte des droits fondamentaux de l'Union européenne et que la protection des données personnelles est regardée aujourd'hui comme un enjeu de souveraineté. La qualification de loi de police étendrait à plusieurs égards leur champ d'application par rapport à ce que permettrait le jeu des règles de conflit. S'agissant des consommateurs, elle permettrait d'écarter l'application des lois étrangères désignées par les conditions générales d'utilisation des sites internet, sans qu'il y ait besoin d'examiner si le site dirige son activité vers le pays de l'internaute (condition prévue par l'article 17.1 du règlement Rome I) ni si l'une ou l'autre des dispositions de la loi étrangère prive le consommateur d'une protection de son droit national (condition prévue par l'article 17.2). Quant aux contrats conclus entre entreprises, par exemple entre un responsable de traitement de données personnelles et un prestataire d'informatique en nuage, ils ne pourraient désigner une autre loi que la loi nationale (ou européenne si le règlement relatif à la protection des données personnelles est adopté). Combinée avec le large champ d'application territorial de la proposition de règlement, qui s'étend aux responsables de traitement établis hors de l'Union européenne lorsque leurs activités sont liées « *à l'offre de biens ou de services à ces personnes concernées dans l'Union* » ou « *à l'observation de leur comportement* » (article 3.2 de la proposition), la qualification

414. Cf. p. ex. M.-L. Niboyet et G. Geouffre de la Pradelle, Droit international privé, L.G.D.J, 2013.

415. L'article 16 du règlement « *Rome 2* » sur la loi applicable aux obligations non contractuelles prévoit une disposition similaire : « *Les dispositions du présent règlement ne portent pas atteinte à l'application des dispositions de la loi du for qui régissent impérativement la situation, quelle que soit la loi applicable à l'obligation non contractuelle* ».

de loi de police garantirait la protection des données personnelles des internautes selon les règles européennes quel que soit le site visité et empêcherait ces sites d'imposer l'application d'autres lois.

Un deuxième corps de règles devant s'imposer à tous les acteurs concernés a trait aux obligations de coopération avec les autorités judiciaires, ainsi qu'avec les autorités administratives procédant à des demandes de données de connexion dans le cadre du code de la sécurité intérieure. L'article 6 de la LCEN, mis en œuvre par le décret n° 2011-219 du 25 février 2011, impose aux hébergeurs de transmettre à l'autorité judiciaire les données « *de nature à permettre l'identification de quiconque a contribué à la création du contenu ou de l'un des contenus des services dont elles sont prestataires* », dans le but d'identifier les auteurs d'infractions pénales. L'article L. 246-1 du code de la sécurité intérieure permet également à l'autorité administrative, dans le cadre des finalités de protection de la sécurité nationale énumérées à l'article L. 241-3 du même code, de leur demander les mêmes données. Or les grandes sociétés américaines ayant la qualité d'hébergeur, telles que *Facebook*, *Twitter* ou *Youtube*, ne s'estiment pas tenues par ces dispositions et répondent à leur guise aux demandes formulées par les autorités, selon des critères qui leur sont propres[416]. Ainsi, *Facebook* indique pour la France dans son *Government Requests Report* que « *nous répondons aux demandes valables concernant des affaires criminelles* » et que « *la légitimité de chacune des demandes que nous recevons est vérifiée, et nous rejetons les demandes trop vagues ou imprécises, ou nous demandons davantage de précisions sur celles-ci* » ; entre juillet et décembre 2013, *Facebook* n'a accédé qu'à 33,9 % des demandes qui lui ont été adressées. La loi actuelle est certes muette sur le champ d'application territorial de l'obligation de coopération des hébergeurs. Il paraît pourtant légitime que des sociétés qui dirigent leur activité vers la France, traitent les données d'internautes français et en retirent un bénéfice commercial soient soumises aux mêmes obligations de coopération que les hébergeurs établis en France en matière pénale et de protection de la sécurité nationale. Rien ne leur interdit d'ailleurs, si elles estiment mal fondées les demandes qui leur sont adressées, de former des recours devant les juridictions judiciaires et administratives compétentes.

La qualification de loi de police est accordée par le juge. Toutefois, cette qualification est facilitée si le texte en cause définit explicitement son champ d'application territorial, prévoit qu'il s'applique nonobstant toute clause contractuelle contraire ou indique dans son exposé des motifs une intention de lui donner la portée d'une loi de police.

(c) La qualification de loi de police permet à un État agissant de manière unilatérale de faire prévaloir sa législation. Dans des matières où la qualification de loi de police n'est pas envisageable, l'application du principe du pays de destination ne peut résulter que d'un accord entre États, soit dans le cadre d'un traité, soit, pour les États membres de l'Union européenne, d'un acte de droit dérivé. En matière de services de médias audiovisuels, le Gouvernement français a exprimé à plusieurs

416. Cf. notamment le rapport précité du groupe interministériel présidé par Marc Robert sur la cybercriminalité.

reprises son souhait de passer du principe du pays d'origine (aujourd'hui prévu par l'article 2 de la directive sur les services de médias audiovisuels, dite *directive SMA*) au principe du pays de destination. L'objectif poursuivi par cette proposition est que tous les services à destination du public français soient soumis au même régime juridique, notamment en matière de soutien à la production et d'exposition des œuvres françaises et européennes. Pour y parvenir, une modification de la directive SMA sera nécessaire.

L'application des règles européennes n'implique pas la localisation des moyens de traitement sur le territoire européen

Dans un contexte marqué par les révélations d'Edward Snowden, il a été proposé d'instaurer une obligation de localisation en Europe des serveurs traitant les données personnelles des Européens, à l'exemple de la règle envisagée par le Brésil dans son projet de « *Marco Civil da internet* ». Outre les difficultés techniques de mise en œuvre, qui semblent avoir expliqué en partie l'abandon de cette disposition dans le texte voté par le Parlement brésilien, une telle règle ne paraît pas apporter un réel renforcement de la protection des données personnelles.

Pour que la protection des données personnelles selon les règles européennes soit effective, deux conditions doivent être réunies : le droit européen doit être applicable et les autorités de contrôle doivent avoir les moyens de veiller à sa mise en œuvre. La localisation physique des moyens de traitement peut servir à déterminer le champ d'application de la règle de protection des données[417], comme c'est le cas aujourd'hui en vertu de l'article 4.1 de la directive n° 95/46/CE, mais ce champ peut aussi être fixé selon d'autres critères, comme le prévoit la proposition de règlement. Sur le plan de la mise en œuvre, la localisation physique sur le territoire n'apparaît pas non plus de nature, en dépit des apparences, à faciliter l'exécution des décisions des autorités de protection des données. Le gestionnaire des serveurs reste de fait libre de procéder comme il le souhaite et notamment de transférer de manière instantanée les données à des serveurs localisés sur d'autres continents. Rien, en particulier, n'empêcherait de fait la société gestionnaire du serveur de transmettre les données à un service de renseignement étranger comme la NSA, si c'est là l'opération que l'on souhaite empêcher. La présence des serveurs sur le territoire ne permettrait pas non plus aux autorités d'intervenir de manière coercitive sur la gestion des données : une telle exécution forcée serait à la fois malaisée sur le plan technique et difficilement envisageable sur le plan juridique. Pour assurer la bonne exécution des décisions des autorités, l'existence de sanctions dissuasives, comme les prévoit la proposition de règlement, apparaît bien plus efficace.

Ces observations ne remettent pas en cause l'intérêt, sur le plan industriel, de soutenir le développement d'acteurs européens de l'informatique en nuage, et l'opportunité qu'il y aurait à fixer de fortes exigences en matière de sécurité des données, que les acteurs européens pourraient être bien placés pour remplir.

417. En outre, même le critère actuel est interprété par les autorités de protection des données de manière large : il ne couvre pas seulement les serveurs installés physiquement sur le sol national, mais aussi les *cookies* enregistrés dans les terminaux des utilisateurs.

2.3.2. Assurer une coopération efficace dans l'application, au sein de l'Union européenne et avec les autres systèmes juridiques

Il revient aux États ou à l'Union européenne de fixer le champ d'application de leurs règles de droit. L'exécution de ces règles par des acteurs issus d'autres États implique en revanche une bonne coopération avec ces derniers. Trois types de relations seront examinées ici : les relations entre États de l'Union européenne, dans la perspective de l'entrée en vigueur de la proposition de règlement relatif à la protection des données personnelles ; les relations entre l'Union européenne et les États-Unis ; les relations avec les autres systèmes juridiques.

La coopération au sein de l'Union européenne

Le passage d'une directive à un règlement relatif à la protection des données personnelles, s'il est accompli, représentera un changement de nature de la règle juridique, qui ne sera plus nationale mais européenne. Les règles de protection des données personnelles sont aujourd'hui fixées par des lois nationales, certes harmonisées par la directive, mais qui ont chacune leur champ d'application défini en fonction du lieu d'établissement du responsable de traitement ; si celui-ci est établi dans plusieurs pays, plusieurs législations nationales lui sont applicables. Si le règlement est adopté, une seule règle de protection s'appliquera dans toute l'Union[418]. Les autorités de protection des données resteront nationales et continueront à exercer leurs pouvoirs sur le territoire de leur État (article 51) mais la proposition de règlement prévoit que si le responsable de traitement est établi dans plusieurs États de l'Union européenne, l'autorité du lieu d'établissement principal[419] est compétente ou, selon les termes votés par le Parlement européen, « *chef de file responsable du contrôle (…) dans tous les États membres* ». Cette disposition, dite de « *guichet unique* », suscite d'importants débats, notamment entre les États membres. Deux craintes principales sont énoncées : le développement de pratiques de « *forum shopping* » des responsables de traitement de données, qui choisiraient comme établissement principal le pays à l'environnement réglementaire le plus favorable ; l'éloignement entre les personnes concernées et l'autorité de protection, qui pourrait même porter atteinte au droit au recours.

La première objection n'est pas dénuée de fondement, si ce n'est que le risque de « *forum shopping* » est en réalité plus grand dans le cadre actuel. Rien n'interdit aujourd'hui à une entreprise de s'établir dans un seul État tout en proposant ses

418. Sous les seules exceptions prévues par le règlement, qui à ce stade renvoie trois sujets importants aux règles nationales : la détermination des obligations légales donnant aux traitements de données un fondement alternatif au consentement de la personne concernée (article 6) ; les cas dans lesquels les traitements doivent être soumis à la consultation préalable des autorités de protection (article 34) ; l'établissement et la fixation du « *statut d'indépendance* » de l'autorité ou des autorités de protection, le contenu de ce statut étant cependant déterminé en grande partie par le règlement (article 49).

419. L'établissement principal est notamment défini comme le lieu « *où sont prises les principales décisions quant aux finalités, aux conditions et aux moyens du traitement de données à caractère personnel* ».

services dans toute l'Union européenne, et de bénéficier ce faisant des différences significatives existant entre les législations nationales. Ainsi, nombre de grandes sociétés sont installées en Irlande, pour des raisons qui tiennent d'ailleurs aussi à la fiscalité. Le règlement instaure une règle européenne unique et réduit donc l'intérêt de ce type de comportement opportuniste. Il demeure certes des possibilités de différence dans l'application des règles par les autorités. Toutefois, les mécanismes de concertation et de cohérence mis en place au sein du Comité européen de protection des données, qui aura des prérogatives renforcées par rapport au G29, paraissent de nature à limiter ce risque. Il pourrait être envisagé, à titre complémentaire, de mettre en place une mutualisation des moyens de contrôle, qui pourrait être utile si des autorités de petits États comme l'Irlande devaient assumer la responsabilité pour toute l'Europe du contrôle de grandes sociétés du numérique.

La seconde difficulté apparaît en revanche plus sérieuse. En vertu de l'article 74 de la proposition de règlement, la personne souhaitant former un recours contre la décision ou la carence d'une autorité de contrôle doit le faire devant les juridictions de l'État de cette autorité, même si elle-même réside dans un autre État. Ce recours, impliquant de s'adresser à un système juridique étranger, dans une langue que la personne peut ne pas connaître, peut être très difficile à exercer. La solution prévue par la proposition de règlement, consistant à permettre à la personne de demander à l'autorité de contrôle de son État d'intenter en son nom un recours contre l'autorité du lieu d'établissement principal, n'est pas satisfaisante. L'autorité de contrôle du pays de la personne est partie prenante, dans le cadre du mécanisme de cohérence (qui implique une concertation préalable à la décision avec l'ensemble des autres autorités), de la décision prise par l'autorité du lieu d'établissement principal. Elle ne peut donc valablement agir au nom de la personne contre cette autre autorité ; une telle situation méconnaîtrait le droit au procès équitable au sens de l'article 6.1 de la Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales.

Une autre solution définie dans le dernier état du projet de règlement serait plus satisfaisante. Elle consiste dans un mode de décision asymétrique : les décisions de sanction à l'encontre d'un responsable de traitement seraient prises par l'autorité chef de file ; en revanche, les décisions de rejet de plainte de particuliers seraient prises par l'autorité du pays du particulier, et le recours serait donc exercé dans ce pays.

Somme toute, la désignation d'une seule autorité compétente pour les traitements paneuropéens apparaît donc comme une nécessité pour assurer l'efficacité de la prise de décision. La procédure coordonnée mise en place à l'encontre de *Google*, si elle illustre les vertus de la coopération au sein du G29, en montre aussi les limites. Sauf à créer une véritable autorité européenne (qui ne résoudrait d'ailleurs pas forcément le problème de l'éloignement entre les personnes et l'autorité), on voit mal quel critère serait mieux justifié que celui du lieu d'établissement principal pour désigner cette autorité unique.

La coopération entre l'Union européenne et les États-Unis

La relation entre l'Union européenne et les États-Unis occupe une place spécifique, en raison de la part des entreprises américaines dans les flux de données et des

régimes *ad hoc* définis en accord avec cet État (*Safe Harbour*, accord PNR, accord TFTP (*Terrorist Finance Tracking Program*) sur le transfert des données financières dans le cadre de la lutte contre le financement du terrorisme) ; de manière plus conjoncturelle, les révélations sur les pratiques des services de renseignement américains ont créé un contexte particulier et ont provoqué une prise de position restrictive du Parlement européen dans sa résolution du 12 mars 2014. Deux questions doivent être résolues : le respect par les entreprises américaines des exigences de protection des données des citoyens européens ; l'accès des autorités américaines aux données des Européens, dans le cadre des lois destinées à assurer la protection de la sécurité nationale des États-Unis. Les deux sujets sont liés, puisque les autorités américaines accèdent aux données des Européens notamment en requérant les entreprises de les leur communiquer, dans le cadre de la section 702 du FISA. Mais il convient de les examiner séparément.

• *Assurer le respect par les entreprises américaines, dans le cadre de leur activité propre, d'un niveau adéquat de protection des données*

La directive n° 95/46/CE énonce un principe simple : un transfert de données personnelles ne peut intervenir vers un pays tiers que si celui-ci assure un « *niveau de protection adéquat* ». Si les États-Unis n'assurent pas un tel niveau, les mécanismes mis en place pour permettre le transfert de données vers ce pays, soit dans un cadre spécifique (décision sur le *Safe Harbour*), soit dans le cadre d'instruments généraux (clauses contractuelles appropriées et règles d'entreprises contraignantes), tendent à la même finalité. C'est au regard de cet impératif de protection qu'il faut envisager la question du traitement des données des Européens par les entreprises américaines.

Une première remarque doit être faite : dès lors que la proposition de règlement élargit le champ d'application des règles européennes, en incluant les responsables de traitement établis hors de l'Union lorsque le traitement, effectué hors de l'Union, est lié à l'offre de biens et de services à des personnes résidant dans l'Union ou à l'observation de leur comportement, la question du respect d'un niveau de protection adéquat ne se pose plus tout à fait dans les mêmes termes[420]. Lorsqu'il sera dans ce champ d'application, le responsable de traitement extra-européen ne devra pas seulement se soumettre aux obligations prévues par les instruments ayant autorisé le transfert (*Safe Harbour*, clauses contractuelles ou règles d'entreprises), mais aussi à l'ensemble des obligations découlant du règlement. Ceci ne retire pas leur utilité aux mécanismes encadrant le transfert, qui comportent notamment des dispositions tendant à s'assurer de la bonne exécution de ses obligations par le responsable de traitement. L'articulation entre champ d'application extraterritorial du règlement et encadrement des transferts gagnerait cependant à être clarifiée par le règlement.

420. Le champ d'application de la directive n° 95/46/CE s'étend déjà à des responsables établis hors de l'Union lorsque les moyens de traitement des données sont situés dans l'Union ; mais puisque les moyens de traitement sont situés dans l'Union, il n'y a pas de transfert. La proposition de règlement crée une situation nouvelle dans laquelle un responsable de traitement établi hors de l'Union qui procède à un transfert de données de résidents européens peut se retrouver *ipso facto* dans le champ d'application de la règle européenne.

Le *Safe Harbour*, qui est le cadre principal du transfert de données vers les entreprises américaines, fait aujourd'hui l'objet de critiques fortes et peu contestées[421]. La communication de la Commission du 27 novembre 2013 relève diverses difficultés : absence de publicité ou publicité insatisfaisante des « *privacy policies* » des entreprises adhérentes au *Safe Harbour*, ce qui méconnaît le droit d'information des personnes concernées et pourrait empêcher la *Federal Trade Commission* (FTC) d'exercer ses prérogatives au titre des pratiques commerciales trompeuses[422] ; incorporation insuffisante des principes du *Safe Harbour* dans les *privacy policies* ; nombreuses fausses revendications d'adhésion au *Safe Harbour*, de la part d'entreprises qui n'ont jamais déposé de dossier d'adhésion auprès du département du commerce ou qui n'ont pas renouvelé leur adhésion ; manque d'information sur les voies de recours des personnes qui estimeraient que les engagements pris par l'entreprise au titre du *Safe Harbour* ont été violés, et manque d'accessibilité de ces voies de recours en raison des frais exigés par certains des organismes gérant les « *modes alternatifs de règlement des différends* » pour lesquels les entreprises peuvent opter[423] ; faiblesse des pouvoirs de sanction des organismes de règlement des différends ; enfin, faible nombre des contrôles exercés par le département du commerce et la FTC. Sur ce dernier point, la responsabilité des autorités européennes apparaît cependant engagée, car elles n'ont adressé aucune plainte à la FTC pendant les dix premières années de fonctionnement du *Safe Harbour*. Certaines améliorations récentes sont relevées par la Commission, comme l'augmentation du taux de rejet des candidatures d'adhésion par le département du commerce et les actions de contrôle engagées par la FTC depuis 2009, qui ont conduit à de lourdes sanctions à l'encontre d'une vingtaine d'entreprises.

Par ailleurs, un renvoi préjudiciel est pendant devant la CJUE, sur la question de savoir si une autorité nationale de protection des données, saisie par un particulier estimant que les pratiques d'un État tiers tel que les États-Unis n'assurent pas une protection adéquate des données personnelles, est liée par la décision de la Commission reconnaissant un niveau de protection adéquat dans cet État. La question, renvoyée par la Haute cour de justice irlandaise, est formulée en termes généraux mais a été posée dans une affaire mettant en cause le *Safe Harbour*.

---

421. Cf. les appréciations convergentes sur ce point de la Commission européenne dans sa communication précitée du 27 novembre 2013 et du Parlement européen dans sa résolution du 12 mars 2014.

422. En effet, la FTC n'est compétente pour s'assurer du respect du *Safe Harbour* qu'au titre de la législation américaine punissant les pratiques commerciales trompeuses. Dès lors, si les entreprises ne rendent pas publics leurs engagements, elles pourraient être à l'abri de telles poursuites.

423. Les entreprises adhérant au *Safe Harbour* ont le choix du mode de règlement des différends avec les personnes dont elles traitent les données : elles peuvent choisir entre le « *panel* » composé de membres des autorités européennes de protection des données (dénommé « *EU Data Panel* ») et des organismes privés, dont certains demandent le paiement de frais aux personnes qui déposent des plaintes.

En dépit de la sévérité de ses constats, les propositions de la Commission tendent seulement à améliorer le système existant sans en remettre en cause les principes fondamentaux. Le système essentiellement déclaratif sur lequel repose le *Safe Harbour* semble pourtant avoir trouvé ses limites. Trois chantiers pourraient être ouverts :

- le passage d'une logique de déclaration d'engagements et d'autocertification à une logique de réglementation contraignante pour les entreprises adhérentes et de certification par des organismes tiers accrédités ;

- sur le fond, l'évolution du contenu des obligations contenues dans le *Safe Harbour*, sujet que n'aborde nullement la Commission alors que ces obligations sont souvent floues et que le renforcement du droit européen que comporterait la proposition de règlement introduirait un écart accru entre les deux cadres ;

- l'intensification des contrôles par les autorités publiques, dans laquelle la FTC paraît prête à s'engager mais qui pourrait être complétée par l'intervention directe d'organismes européens, comme c'est le cas dans d'autres accords conclus avec les États-Unis comme le TFTP (*Terrorist Finance Tracking Program*).

La position de départ de la Commission dans la négociation avec les États-Unis n'apparaît pas suffisamment ambitieuse. Les entreprises américaines ont besoin du *Safe Harbour* : le marché européen, qui compte 500 millions d'internautes, est pour elles le plus important au monde, les internautes européens étant plus nombreux que les internautes américains et le taux de pénétration étant bien supérieur en Europe à ce qu'il est en Chine. Elles pourraient continuer à traiter des données personnelles des Européens en l'absence du *Safe Harbour*, sur la base de fondements alternatifs (consentement indubitable de la personne, clauses contractuelles appropriées ou règles d'entreprises contraignantes), mais leurs opérations en seraient rendues plus difficiles.

• *Limiter l'accès des autorités américaines aux données personnelles des Européens aux fins de sécurité nationale et l'entourer de garanties négociées*

Le problème de l'accès des autorités américaines aux données personnelles des Européens ne se pose pas dans les mêmes termes. L'Union européenne et ses États membres sont en droit de définir souverainement, de manière unilatérale, les conditions dans lesquelles doivent s'effectuer l'accès d'entreprises étrangères aux données personnelles de leurs citoyens. S'agissant de l'accès d'un État tiers à ces données, les autorités européennes ont le droit et le devoir d'exiger la protection des droits fondamentaux de leurs citoyens ; mais cet État tiers, en l'occurrence les États-Unis, a aussi des droits en tant que souverain de prendre les mesures qu'il estime nécessaires pour garantir sa sécurité nationale. Une telle question, qui concerne les rapports entre États souverains relève du droit international public. Elle pourrait d'ailleurs relever de la compétence de la Cour internationale de justice, si les États-Unis en reconnaissaient la juridiction, ce qui n'est pas le cas[424].

424. Sauf dans le cadre de la convention de Vienne du 18 avril 1961 sur les relations diplomatiques, ratifiée par les États-Unis et dont un protocole prévoit la compétence de la CIJ pour régler les différends relatifs à sa mise en œuvre. Sur l'hypothèse d'une saisine de la

L'espionnage est en droit international public dans une situation paradoxale. La majeure partie de la doctrine s'accorde à reconnaître qu'aucune norme de droit international public, ni conventionnelle ni coutumière, n'interdit en tant que tel l'espionnage en temps de paix[425]. Selon le principe constant affirmé depuis l'affaire du *Lotus*[426], « *les limitations à l'indépendance des États ne se présument pas : en l'absence de règles prohibitives venant limiter sa liberté, chaque État reste libre d'adopter les principes qu'il juge les meilleurs et les plus convenables* »[427]. Or, aucune convention internationale ne prévoit l'interdiction de l'espionnage en temps de paix, et le fait que de très nombreux États se livrent à cette pratique empêche de reconnaître l'existence d'une coutume contraire. Mais il est également constant que les États sanctionnent pénalement dans leur ordre interne, souvent de manière très lourde, les activités d'espionnage[428]. La plupart des affaires d'espionnage qu'a connu l'histoire des relations internationales se sont d'ailleurs traduites par la punition des espions appréhendés et par une absence de réaction, autre que de l'ordre de la protestation à caractère politique, sur le plan des relations entre États. Cette double nature de l'acte d'espionnage, toléré en droit international public même s'il est considéré comme inamical, mais puni en droit interne, a été notamment reconnue par la Cour fédérale de justice allemande (*Bundesgerichtshof*) dans un arrêt du 30 janvier 1991.

Les programmes mis en œuvre par les États-Unis dans le cadre de la section 702 du FISA sont toutefois d'une autre envergure que les activités ponctuelles d'espionnage sur lesquelles la jurisprudence et la doctrine internationales ont pu jusqu'ici prendre position. Dans un article de 1960, les professeurs Gérard Cohen-Jonathan et Robert Kovar avançaient l'idée que si l'espionnage en tant que tel n'était pas interdit par le droit international public, l'entretien d'un service régulier d'espionnage sur le territoire d'un autre État pourrait, par son caractère systématique, être considéré comme une violation de la souveraineté de celui-ci ; or c'est bien le caractère systématique de la collecte de renseignements qui est ici en cause. En outre, certains aspects des pratiques des services de renseignement américains, comme la violation du secret des correspondances diplomatiques (interdite par une norme expresse du droit international public, la convention de Vienne du 18 avril 1961), l'écoute de chefs d'États étrangers en dehors de tout contexte de tension dans les relations avec ces États et les efforts délibérés d'affaiblissement de la sécurité des communications électroniques cryptées, soulèvent des interrogations particulières. Enfin, l'ampleur de la réprobation internationale, manifestée par l'adoption de résolutions de l'Assemblée générale

---

CIJ dans l'affaire *Prism* en raison des allégations d'écoute de communications diplomatiques, cf. R. Bismuth, « La diplomatie française sur écoute : la Cour internationale de justice est une option », *Le Monde*, 28 octobre 2013.

425. Cf. pour une revue très complète F. Lafouasse, « L'espionnage en droit international », *Annuaire français de droit international*, volume 47, 2001, pp. 63-136.

426. Cour permanente de justice internationale (CPJI), 1927.

427. P. Weil, « Le droit international public en quête de son identité. Cours général de droit international public », *RCADI*, tome 237 (1992- VI), Martinus Nijhoff Publishers, 1996, p. 210.

428. Cf. en France les articles 411-1 et suivants du code pénal.

des Nations unies[429], du Comité des ministres et de l'Assemblée parlementaire du Conseil de l'Europe, du Parlement européen, le texte final de la conférence *Net Mundial* de Sao Paulo[430], ainsi que par les prises de position des autorités de très nombreux États de par le monde, pourrait traduire l'émergence d'une coutume prohibant la collecte massive de données personnelles par l'interception des communications internationales.

Dans cette optique, les États européens seraient fondés en droit à adopter des contre-mesures (c'est-à-dire des mesures prises en rétorsion à une violation du droit international public). Celles-ci peuvent consister à mettre fin à une doctrine de non-espionnage, comme l'a envisagé l'Allemagne[431]. Elles peuvent aussi tendre à assurer la protection des droits des citoyens européens, en restreignant les transferts de données personnelles vers les entreprises qui ne s'engageraient pas à refuser l'accès des autorités américaines à ces données.

Les instruments juridiques actuels ne sont pas très explicites sur les conditions dans lesquelles les autorités d'États tiers peuvent accéder, à des fins judiciaires ou de protection de leur sécurité nationale, aux données personnelles ayant fait l'objet d'un transfert vers un acteur établi dans cet État tiers. La décision du 26 juillet 2000 de la Commission établissant le *Safe Harbour* prévoit que « *l'adhésion aux principes peut être limitée par (…) les exigences relatives à la sécurité nationale, l'intérêt public et le respect des lois des États-Unis* ». Les clauses contractuelles type prévoient que l'importateur des données (c'est-à-dire l'acteur établi en dehors de l'Union européenne) doit prévenir l'exportateur (c'est-à-dire l'acteur établi dans l'Union européenne) de toute demande légalement contraignante de transmission des données personnelles qui lui est adressée, sauf si une obligation juridique lui interdit de communiquer cette information. Il en ressort assez nettement qu'aucun de ces instruments ne limite la capacité des importateurs de données à les transmettre aux autorités judiciaires ou administratives de leur État lorsqu'elles sont requises de le faire.

À la suite des révélations qui ont débuté en juin 2013, le Parlement européen s'est particulièrement inquiété de cette situation. L'un de ses principaux motifs de préoccupation tient au développement de l'informatique en nuage, dont les prestataires les plus importants sont américains ; les données personnelles des Européens, y compris celles traitées par leurs organismes gouvernementaux, sont de plus en plus souvent confiées à des organismes tenus de les transmettre aux autorités américaines lorsque celles-ci le demandent. Il a donc adopté dans le cadre de la proposition de règlement relative à la protection des données personnelles un article 43 *bis* beaucoup plus restrictif que les dispositions actuelles. Il prévoit notamment les dispositions suivantes :

---

429. Résolution n° 68/167 du 18 décembre 2013, « Le droit à la vie privée à l'ère du numérique ».

430. Global Multistakeholder Meeting on the Future of Internet Governance, "NETMundial Multistakeholder Statement", 24 avril 2014.

431. « Striking back. Germany Considers Counterespionage Against US », *Der Spiegel*, 18 février 2013.

- Aucun responsable de traitement ou sous-traitant[432] n'a le droit de mettre en œuvre une décision judiciaire ou administrative d'un État tiers lui enjoignant de communiquer des données, sauf s'il existe un traité d'entraide juridique mutuelle ou un autre accord international entre cet État tiers et l'Union européenne ou un État membre.

- Le responsable de traitement ou le sous-traitant doit obtenir l'accord préalable de l'autorité de protection des données compétente ; celle-ci examine si la demande répond aux conditions fixées par l'article 44, c'est-à-dire si le transfert de données est nécessaire pour des motifs importants d'intérêt général reconnus par le droit de l'Union ou à la constatation, à l'exercice ou à la défense d'un droit en justice.

- Le responsable de traitement ou le sous-traitant doit informer les personnes concernées de la demande de l'État tiers et de la suite qui y a été donnée par l'autorité de protection des données.

L'article 43 *bis* suscite plusieurs interrogations. Tout d'abord, il met les entreprises concernées dans une situation de conflit insurmontable entre leurs obligations au titre de la législation de l'État tiers et celles prévues par le droit de l'Union européenne. Aucun État ne peut accepter que les décisions de ses autorités judiciaires ou des administrations chargées de la protection de sa sécurité nationale soient soumises à l'approbation d'une autorité publique étrangère. Dans le cas de la collecte de renseignement, intervient en outre l'obstacle du secret de la défense nationale, qui exclut toute communication du type de celles prévues par l'article 43 *bis*. Si une telle disposition était adoptée, les entreprises américaines concernées ne pourraient probablement pas s'y soumettre. En second lieu, il aborde de manière très large un problème qui n'a trait qu'à la collecte de renseignement par les États-Unis et le cas échéant par quelques autres États associés à celle-ci dans le cadre du programme dit « *Five Eyes* »[433].

L'étude préconise sur ce point une solution alternative, permettant à la Commission européenne, dans le cadre du règlement, de restreindre au cas par cas les transferts de données vers les autorités administratives ou judiciaires d'États tiers, lorsque ces autorités se livrent à une collecte de données manifestement abusive ou ne respectent pas les standards de l'État de droit (cf. *infra* 3.5.2).

La coopération avec les autres systèmes juridiques

Si la relation avec les États-Unis revêt une importance particulière, elle ne doit pas occulter les besoins et les opportunités de coopération avec d'autres systèmes

432. Il s'agit du terme employé par le règlement pour désigner les acteurs traitant les données pour le compte du responsable de traitement ; cette notion couvre notamment les prestataires d'informatique en nuage.

433. Il s'agit, outre le Royaume-Uni qui ne relève pas du sujet traité ici puisqu'il est membre de l'Union européenne, du Canada, de l'Australie et de la Nouvelle-Zélande. La Commission a décidé que le Canada et la Nouvelle-Zélande assuraient un niveau de protection adéquat des données personnelles, qui peuvent donc leur être librement transférées. Dans sa résolution du 12 mars 2014, le Parlement européen a demandé à la Commission de réexaminer ces décisions.

juridiques, qu'il s'agisse d'organiser la protection des données personnelles, de renforcer la lutte contre la cybercriminalité ou de définir des principes de gouvernance au niveau mondial.

(a) L'Union européenne n'est pas isolée dans sa vision exigeante de la protection des données à caractère personnel. La convention n° 108 du Conseil de l'Europe rassemble la quasi-totalité des États européens, bien au-delà de la seule Union européenne. Au cours des dernières années, des pays membres du G20 tels que la Corée du sud puis le Brésil se sont dotés de législations ambitieuses. Le *Personal Information Protection Act* de 2011 de la Corée du sud impose ainsi la désignation d'un agent responsable de la protection des données (l'équivalent du délégué à la protection des données personnelles de la législation européenne) par tous les organismes publics et privés impliqués dans la collecte de celles-ci. La loi prévoit l'obligation de recueillir le consentement de la personne, de préciser les finalités de la collecte, la limitation de la durée de conservation ; elle va même plus loin que le droit de l'Union européenne en interdisant le refus d'un service à une personne au motif que celle-ci n'accepterait pas la communication de ses données, au-delà d'une liste d'informations minimales pouvant légalement être demandées. Sans aller tous jusqu'à ce niveau d'exigence, les États membres de l'APEC (*Asia Pacific Economic Cooperation*) se sont dotés de principes communs. L'existence d'une Conférence internationale des autorités de protection des données permet d'entreprendre des actions à l'échelle mondiale, comme cela a été le cas au sujet des *Google Glass* en 2013.

L'exemple de la *Marco Civil da Internet*

Ayant l'ambition d'être la « *constitution* » de l'internet au Brésil, la *Marco Civil da internet* aborde de nombreux sujets ayant trait aux droits fondamentaux.

L'article 7 reconnaît les droits suivants aux utilisateurs d'internet : l'inviolabilité de la correspondance, sauf sur décision judiciaire ; le droit à ne pas voir suspendue leur connexion à internet, sauf en raison d'une dette envers le fournisseur d'accès ; le droit à ce que leurs données personnelles ne soient pas diffusées à des tiers, sauf en vertu de leur consentement exprès et informé ou pour un motif prévu par la loi.

L'article 8 prévoit la nullité des clauses contenues dans un contrat d'adhésion relatif à un service rendu sur internet qui écarteraient la compétence de la juridiction brésilienne.

L'article 9 est relatif à la neutralité d'internet. Il la définit de manière stricte, en n'admettant de dérogations que pour des raisons liées à la gestion du trafic ou pour acheminer des services d'urgence.

L'article 11 dispose que la loi brésilienne est applicable à tout opérateur quel que soit son lieu d'établissement, dès lors qu'il traite les données personnelles de Brésiliens.

Les articles 18 et 19 limitent la responsabilité des fournisseurs d'accès et d'applications pour les contenus générés par des tiers.

Ces évolutions permettent d'envisager une politique plus ambitieuse de reconnaissance mutuelle et d'actions conjointes. L'Union européenne pourrait engager la libéralisation des transferts de données avec les seuls systèmes juridiques dont elle reconnaît le caractère équivalent du niveau de protection. À cet égard, le système de décisions de la Commission prévu par la directive n° 95/46/CE et que la proposition de règlement envisage de reconduire n'est peut-être pas l'instrument le plus adapté, car il permet seulement la libéralisation des transferts de données vers l'État tiers, sans garantie que celui-ci procède à une reconnaissance mutuelle en faveur de l'Union européenne. La signature de conventions entre l'Union européenne et l'État tiers, le cas échéant dans un cadre *ad hoc* à définir par le règlement, pourrait être préférable. Les actions conjointes des autorités de protection des données pourraient se concentrer sur des acteurs opérant à l'échelle mondiale ou sur des phénomènes émergents. Enfin, un instrument mondial contraignant en matière de protection des données, sur la base de la résolution de Madrid de la Conférence internationale des autorités de protection de 2009, pourrait être mis à l'étude. La convention n° 108 du Conseil de l'Europe, ouverte à la signature d'États tiers mais par hypothèse centrée sur l'Europe n'est en effet pas appropriée à cet objectif.

(b) Le rapport du groupe de travail interministériel sur la cybercriminalité a mis en évidence les lenteurs et les pesanteurs encore trop grandes de la coopération internationale en la matière. Les accords d'entraide judiciaire traditionnels n'apparaissent pas adaptés, en raison de la complexité des procédures qu'ils impliquent, au traitement de ce phénomène. Il apparaît donc souhaitable de faire de la lutte contre la cybercriminalité une priorité de la politique de coopération pénale internationale, en développant par des instruments *ad hoc* des mécanismes d'échanges rapides dans la collecte des preuves et la reconnaissance des décisions. La lutte contre les « cyberparadis », notoirement connus pour héberger des activités de cyberdélinquance en raison de la tolérance des autorités locales, devrait également s'intensifier. À l'exemple des initiatives prises au cours des dernières années en matière de lutte contre le financement du terrorisme et les paradis fiscaux, un groupe d'action interétatique pourrait être mis en place, définissant des recommandations détaillées sur les pratiques de coopération à mettre en place et publiant des listes d'États non coopératifs.

2.3.3. Remédier aux insuffisances du mode actuel de gouvernance d'internet

Un mode de gouvernance qui ne fait pas consensus

Le mode de gouvernance actuel de l'internet est loin de faire consensus au niveau mondial et présente des insuffisances importantes. Il est, en effet, la cible de critiques diverses, les unes relatives à l'inclusion d'acteurs non étatiques, les autres portant sur son caractère insuffisamment démocratique.

Ces critiques proviennent en premier lieu d'États (notamment la Chine et la Russie) qui ne reconnaissent pas la légitimité d'un modèle dans lequel la société civile et les entreprises siègent à côté de représentants des gouvernements. Cette

opposition frontale au modèle multiacteurs les conduit à promouvoir à l'échelle internationale la mise en place d'un système exclusivement intergouvernemental : en 2011, l'Organisation de coopération de Shanghaï (Chine, Russie, Kazakhstan, Kirghizistan, Ouzbékistan, Tadjikistan) a ainsi déposé à l'ONU une proposition de « *code de conduite* » intergouvernemental ; au même moment, l'Inde, le Brésil et l'Afrique du sud proposaient la création d'un Comité des Nations Unies pour les politiques relatives à internet (CIRP), dont le mandat aurait inclus la « *coordination et la supervision des structures responsables du fonctionnement technique et opérationnel d'Internet* »[434]. Aucune de ces propositions n'a toutefois abouti, pas plus que la proposition émise fin 2012 par ces mêmes États de confier la gestion technique de l'infrastructure d'Internet à l'Union internationale des télécommunications[435]. Il reste que la nature même du modèle multiacteurs est loin de faire consensus à l'échelle internationale.

Ces critiques proviennent en second lieu d'États (notamment au sein de l'Union européenne) qui soulignent le caractère insuffisamment démocratique de ce modèle de gouvernance. Elles procèdent du constat selon lequel le modèle multiacteurs s'est avéré efficace pour gérer le développement exponentiel du réseau Internet, mais qu'il doit être amendé afin d'assurer une meilleure représentation des différentes parties prenantes et une meilleure prise en compte de l'intérêt général. La Commission européenne plaide à cet égard en faveur d'une gouvernance plus transparente, reposant sur une représentation équilibrée des différentes parties prenantes et dans laquelle les organes décisionnels seraient davantage responsabilisés, ce qui implique qu'ils puissent être contraints de rendre des comptes aux États[436]. Ces préconisations de la Commission européenne font directement écho aux principes adoptés par l'ensemble des participants au forum *Netmundial* organisé à Sao Paulo les 23 et 24 avril 2014 à l'initiative de la présidente Dilma Rousseff. Parmi ces principes figurent en effet la transparence, la responsabilisation et le caractère équitable de la représentation des différentes parties prenantes[437]. Bien qu'elles concernent la gouvernance de l'infrastructure d'Internet au sens large, il convient de préciser que ces positions ont largement trait au fonctionnement de l'ICANN dont de nombreux États, notamment la France, considèrent qu'elle fonctionne de manière insuffisamment transparente. Elle ne tient ainsi pas suffisamment compte des positions exprimées par les États dans son processus de décision[438], en dépit de la création d'un *Government Advisory*

434. V. B. de la Chapelle, 2012, *op.cit.*

435. Ce sujet était à l'ordre du jour du sommet de l'UIT à Dubaï (3-14 décembre 2012) et a entraîné une forte polarisation des positions entre les pays émergents d'une part, les États-Unis et l'Union européenne d'autre part.

436. V. *Politique et gouvernance de l'Internet : le rôle de l'Europe à l'avenir*, COM/2014/072 final, Communication de la Commission au Parlement européen, au Conseil, au Comité économique et social européen et au Comité des régions, 2014 : http://eur-lex.europa.eu/legal-content/FR/ALL/?uri=CELEX%3A52014DC0072

437. V. Déclaration de principes adoptée à l'issue du sommet Netmundial : http://netmundial.br/wp-content/uploads/2014/04/NETmundial-Multistakeholder-Document.pdf

438. V. pour une analyse critique et particulièrement précise du fonctionnement de l'ICANN : *A Constitutional Solution for Internet Governance,* R. H. Weber et R. S. Gunnarson, *The*

Committee (GAC) au sein duquel les gouvernements sont représentés. Là encore, ces positions montrent que le modèle multiacteurs suscite d'importantes réserves, y compris parmi les États qui le soutiennent au détriment d'un modèle strictement intergouvernemental.

Cette critique du modèle multiacteurs se double d'une remise en question des liens entre les organisations chargées de la gouvernance de l'infrastructure d'Internet et le gouvernement américain.

De manière structurelle, cette remise en cause tient au déplacement du centre de gravité du réseau internet hors des États-Unis[439] : la majorité des utilisateurs du réseau se trouvent désormais en Asie, en Amérique latine et en Afrique, et cette tendance est appelée à s'accentuer[440]. De manière conjoncturelle, les révélations d'Edward Snowden relatives aux programmes de surveillance mis en œuvre par les États-Unis[441], bien qu'elles ne concernent pas directement les organisations chargées de la gouvernance de l'infrastructure d'Internet, ont conduit de nombreux acteurs à interroger la tutelle de fait exercée par les États-Unis envers ces organisations. Depuis lors, de nombreuses voix se sont élevées pour dénoncer cette tutelle ; tel fut par exemple le cas de la présidente Dilma Rousseff lors de l'ouverture de la 68e session de l'Assemblée générale des Nations Unies le 24 septembre 2013[442]. Ces appels ne sont pas restés sans effet : le 14 mars 2014, l'administration des États-Unis a annoncé son intention de ne plus assurer la supervision du Système de noms de domaines[443] et de la confier à une instance globale multiacteurs. La forme institutionnelle et juridique que prendra cette dernière instance reste toutefois à définir.

Columbia Science and Technology Law Review, vol. XIV, 2012 : http://www.stlr.org/html/volume14/WeberGunnarson.pdf

439. V. pour une analyse américaine de cette question : *Defending an Open, Global, Secure and Resilient Internet*, Council on Foreign Relations, Independent Task Force Report n° 70, 2013. P. 4 : « *For the past four decades, the United States was the predominant innovator, promoter and shaper of cyberspace, but the window for US leadership is now closing. In Asia, Latin America, and Africa, the number of networked users is rapidly increasing. Cyberspace is now becoming reflective of the world's Internet users* ».

440. Au 30 juin 2010, on dénombrait : 825 Ms d'utilisateurs en Asie, 475 Ms en Europe, 266 Ms en Amérique du Nord, 205 Ms en Amérique latine, 111 Ms en Afrique, 63 Ms au Moyen-Orient (*Le dessous des cartes*, J.-C. Victor, Tallandier, 2012).

441. V. le site du *Guardian*, sur lequel a été diffusé l'ensemble des révélations d'Edward Snowden : http://www.theguardian.com/world/the-nsa-files

442. V. l'intervention de la présidente Dilma Rousseff : http://gadebate.un.org/sites/default/files/gastatements/68/BR_en.pdf

443. V. annonce de la National Telecommunications and Information Administration (NTIA), « NTIA announces Intent to Transition Key Internet Domain Name Functions », 14 mars 2014 : http://www.ntia.doc.gov/press-release/2014/ntia-announces-intent-transition-key-internet-domain-name-functions

Un mode de gouvernance qui peine à faire face à certains défis majeurs pour l'avenir du réseau

À ces critiques s'ajoute le constat d'une certaine incapacité du mode actuel de gouvernance d'Internet à faire face à des défis majeurs pour l'avenir du réseau.

L'un de ces défis majeurs a trait à la question de la rareté des adresses Internet[444]. Contrairement à une idée reçue, le stock d'adresses disponibles sur internet est en effet limité : dans le cadre de la quatrième version du protocole internet (IPv4), c'est à dire la plus utilisée à l'échelle mondiale, ce stock comprend par exemple 4,3 milliards d'adresses composées chacune d'un numéro à 32 chiffres. Si ce nombre pouvait apparaître suffisant lors du lancement d'IPv4, il ne l'est plus aujourd'hui compte tenu du développement exponentiel du réseau et de son extension à l'Internet des objets : ainsi, depuis septembre 2012, il n'existe en théorie plus d'adresses disponibles sous IPv4 pour faire face à la demande[445]. L'enjeu consiste dès lors à organiser la migration des utilisateurs d'IPv4 vers une nouvelle version du protocole Internet, à savoir la sixième version de celui-ci (IPv6) qui comprend un nombre d'adresses très nettement supérieur (chaque adresse comprenant 128 chiffres). Or si la plupart des acteurs internationaux – États, sociétés civiles, organisations en charge de la gouvernance des infrastructures d'Internet – s'accordent sur la nécessité à terme de conduire à son terme cette migration, aucun instrument n'a, à ce jour, permis de la lancer pleinement. Un chiffre résume ce blocage : en octobre 2011, seuls 3% des noms de domaine étaient compatibles avec IPv6[446]. Deux raisons expliquent cette situation : l'absence, à l'échelle internationale, d'une organisation centrale susceptible de conduire cette migration au moyen d'instruments juridiques contraignants ; l'absence d'incitations des acteurs privés (notamment les fournisseurs d'accès à Internet) à opérer cette migration, dont les coûts de transition devraient s'avérer élevés compte tenu de la non-interopérabilité entre IPv4 et IPv6[447]. À cet égard, cet exemple est symptomatique des limites du droit souple en matière de gouvernance des infrastructures d'Internet.

---

444. V. pour une présentation détaillée des enjeux relatifs à cette question : *Internet Fragmentation, Highlighting the Major Technical, Governance and Diplomatic Challenges for US Policy Makers*, J. F. Hill, Havard University, 2012.

445. V. B. du Marais, 2013, *op. cit.*

446. V. J. F. Hill, 2012, *op. cit.*

447. Cf. Audition de M. Weill, directeur général de l'AFNIC, 23 mai 2014.

Mettre le numérique au service des droits individuels et de l'intérêt général

Les habitudes de consentement passif des individus semblent parfois l'un des principaux obstacles à une protection effective des droits fondamentaux dans les usages numériques. Ainsi, les conditions générales d'utilisation sont invariablement acceptées sans pour autant être lues. Dans la majorité des cas, les utilisateurs d'une application ne modifient pas les réglages par défaut des paramètres de confidentialité. Les retraits de contenus opérés par les plateformes ne donnent lieu qu'à bien peu de plaintes. L'Union européenne peut bien renforcer les droits des utilisateurs en imposant le passage de « *l'opt-out* » (droit de s'opposer) à « *l'opt-in* » (obligation de recueil du consentement) pour l'installation des *cookies*[448] : les internautes poursuivent imperturbablement leur navigation. L'ignorance des enjeux de protection des données personnelles ou de liberté d'expression n'est pas seule en cause : nombre des personnes auditionnées dans le cadre de cette étude, pourtant particulièrement au fait de ces questions, ont confessé se comporter de la sorte. Bien souvent, les internautes savent que leurs données personnelles seront largement disséminées et réutilisées ; et pourtant ils cliquent.

Cette attitude est en réalité rationnelle, dans la mesure où les droits actuels ne donnent que très peu de pouvoirs aux individus. À quoi bon lire les politiques relatives à la confidentialité ou aux contenus pouvant être mis en ligne, puisqu'elles sont de toute façon imposées à tous les utilisateurs du service, sans aucune marge de négociation pour ces derniers? Les individus peuvent certes choisir de ne pas recourir au service ou de l'abandonner ; mais le recours à des services concurrents conduirait à la même situation. La plus-value du droit par rapport au simple jeu du marché est ici bien mince.

448. Modification prévue dans le cadre du « *troisième paquet télécoms* » par la directive n° 2009/136/CE du 25 novembre 2009 et transposée en France par l'ordonnance n° 2011-1012 du 24 août 2011 (la disposition figure au II de l'article 32 de la loi du 6 janvier 1978).

Aujourd'hui, les droits reconnus aux individus se limitent, pour l'essentiel, à leur permettre de rester à l'écart du traitement de leurs données (choix qui n'est presque jamais fait), sans leur donner de réel pouvoir sur le contenu du service et la manière dont leurs données sont traitées. Mettre le numérique au service des droits individuels, tel devrait être le premier principe directeur de la protection des droits fondamentaux dans les usages numériques. Nombre des propositions formulées ci-après tendent donc à accroître les capacités d'action des individus (par exemple en promouvant les technologies de protection de la vie privée, en accroissant la transparence sur les classements proposés par les plateformes, en créant un droit d'alerte en matière de protection des données personnelles ou en consacrant le droit de faire valoir ses observations face à l'application d'un algorithme prédictif) ou de leurs groupements (en créant une action collective en matière de protection des données personnelles, en mettant en *open data* l'ensemble des déclarations transmises à la CNIL ou en poussant à la délibération des politiques de contenus des plateformes). Par cette logique « *d'empowerment* », « *d'autonomisation* » des individus, l'intervention publique peut accroître la capacité des individus à agir pour la défense de leurs droits et à amplifier ainsi les possibilités d'action des pouvoirs publics eux-mêmes. Face à des acteurs du numérique dont le succès passe par leur relation privilégiée avec leurs utilisateurs, les pouvoirs publics doivent eux aussi savoir « *s'allier avec la multitude* »[449]. Le potentiel d'innovation du numérique, loin d'être bridé, s'en trouvera, de surcroît, renforcé.

Le second principe directeur des propositions formulées dans cette troisième partie tend à mettre le numérique au service de l'intérêt général. Le numérique peut bénéficier de manière considérable à l'efficacité des politiques de santé, d'éducation, de sécurité, de lutte contre la fraude ou de culture, ainsi qu'à la simplification des démarches administratives ; encore faut-il que les personnes publiques disposent de cadre et d'instruments juridiques appropriés pour saisir ces opportunités, tout en assurant le respect des droits individuels. Il s'agit pour elles de concilier des droits fondamentaux entre eux ou des libertés avec des objectifs de valeur constitutionnelle : ainsi de la sûreté à laquelle concourent la prévention et la répression des crimes les plus graves. Le Conseil d'État propose en ce sens de mieux affirmer la liberté de réutilisation statistique des données personnelles, d'ouvrir de manière maîtrisée l'utilisation des numéros d'identification, de renouveler la conception des garanties du pluralisme dans les médias, de renforcer les garanties entourant l'usage des fichiers de police et la prévention des atteintes à la sécurité nationale ou encore de rééquilibrer la gouvernance d'internet pour mieux y faire valoir les intérêts généraux que notre société entend protéger et a consacrés par la loi.

Deux remarques préalables doivent être faites.

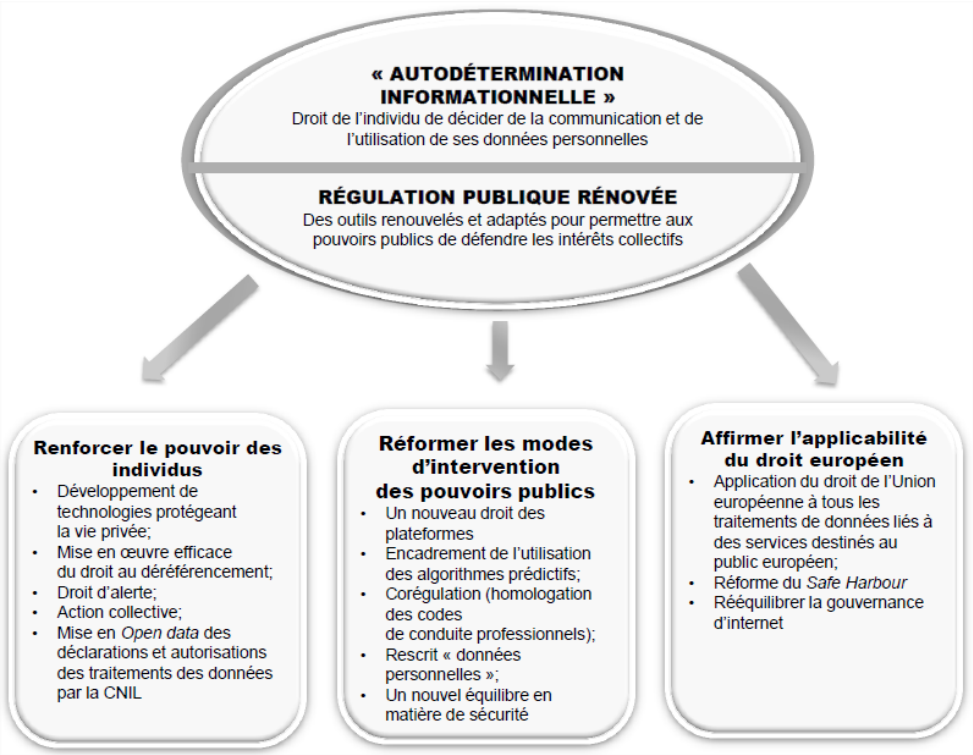
En premier lieu, même s'il reste un espace d'action autonome pour le droit interne, soit par la norme législative ou réglementaire, soit par le droit souple, nombre des propositions de cette étude relèvent de la compétence des institutions de l'Union européenne, soit parce qu'elles nécessitent une modification du droit de l'Union existant, soit parce que l'Union européenne constitue le niveau pertinent d'action.

449. Selon la formule de N. Colin et d'H. Verdier, *L'âge de la multitude*, *op. cit*.

Le projet de règlement relatif à la protection des données personnelles, en particulier, sera déterminant pour la faisabilité de plusieurs propositions majeures, qui sont donc destinées aux autorités françaises chargées des négociations sur ce texte. D'autres propositions relèvent des prérogatives du G29 (proposition n° 5) ou de la Commission européenne (proposition n° 43). Enfin, certaines impliquent de nouvelles propositions de directives, dont le Gouvernement français pourrait soumettre l'idée à la Commission européenne et aux autres États membres de l'Union européenne (proposition n° 6).

En second lieu, le Conseil d'État s'est attaché à inscrire ses propositions dans la trajectoire de maîtrise des dépenses publiques dans laquelle la France s'est engagée. Seul le nécessaire renforcement des moyens des autorités de contrôle que sont la CNIL et la CNCIS ont une incidence limitée sur les dépenses publiques.

Le schéma ci-dessous présente de manière synoptique les orientations privilégiées par l'étude en réponse notamment à l'analyse des risques illustrée dans le schéma figurant au 2.1.1 (p. 164).



Source : Conseil d'État, section du rapport et des études

3.1. Définir les principes fondant la protection des droits fondamentaux à l'ère du numérique

3.1.1. Le droit sur les données personnelles : un droit à l'autodétermination plutôt qu'un droit de propriété

Face aux limites du cadre actuel de la protection des données à caractère personnel, il est parfois proposé[450] de donner aux individus un véritable droit de propriété sur leurs données ; le but recherché est notamment de susciter une implication plus active, les individus devenant financièrement intéressés à une bonne gestion de leurs données. Le Conseil d'État ne recommande pas d'emprunter cette voie en dépit de son attrait apparent. S'il convient en effet de renforcer la dimension de l'individu acteur dans le droit à la protection des données, c'est en envisageant celui-ci comme un droit à l'autodétermination plutôt que comme un droit de propriété.

Ecarter l'introduction d'une logique patrimoniale dans la protection des données personnelles

En l'état du droit, il n'existe pas de droit de propriété de l'individu sur ses données personnelles. Comme le soulignait déjà en 2002 un rapport du président Pierre Truche[451], la protection des données personnelles, telle qu'elle est conçue par la loi du 6 janvier 1978, la convention n° 108 du Conseil de l'Europe ou la directive n° 95/46/CE, ne repose pas sur une logique patrimoniale mais sur une logique de droits attachés à la personne. Le code de la propriété intellectuelle reconnaît un droit de propriété au producteur d'une base de données lorsque la constitution de la base « *atteste d'un investissement financier, matériel ou humain substantiel* »[452] ; il n'existe pas en revanche de droit de propriété sur les données brutes.

Si le droit de propriété de l'individu sur ses données n'existe pas aujourd'hui, il pourrait être créé demain. Selon la formule constante du Conseil constitutionnel, « *les finalités et les conditions d'exercice du droit de propriété ont connu depuis 1789 une évolution caractérisée par une extension de son champ d'application à des domaines nouveaux* »[453] ; la reconnaissance d'un droit de propriété de l'individu sur ses données ne représenterait donc qu'une nouvelle extension. Elle impliquerait une intervention du législateur, puisque seraient en cause les « *principes fondamentaux du régime de la propriété* » au sens de l'article 34 de la Constitution.

---

450. Cf. par exemple L. Lessig dans la première édition de *Code is Law ;* la seconde édition est nettement plus nuancée, l'auteur ayant choisi de tenir compte des critiques formulées à l'encontre de cette proposition. En France, cf. les positions d'A. Bensoussan dans CNIL, «Vie privée à l'horizon 2020. Paroles d'experts», *Cahiers IP Innovation et prospective, n° 1* et de Pierre Bellanger « La souveraineté numérique » janvier 2014, Stock, p. 201 et suiv.

451. P. Truche, J.-P. Faugère et P. Flichy, *Administration électronique et protection des données personnelles. Livre blanc*, février 2002.

452. Article L. 341-1 du code de la propriété intellectuelle.

453. Cf. notamment la décision n° 2009-580 DC du 10 juin 2009, § 13.

Plusieurs arguments sont invoqués en faveur de la reconnaissance d'un tel droit. Le principal est sans doute que les bases de données personnelles font aujourd'hui l'objet d'une appropriation généralisée, dans le cadre de l'économie marchande présentée ci-dessus (cf. 2.1.1) : les acteurs économiques jouissent d'un droit de propriété sur les bases de données personnelles, alors que les personnes répertoriées dans ces bases ne sont pas propriétaires de leurs données, ce qui peut sembler paradoxal. Reconnue dans son droit de propriété, la personne verrait sa position renforcée à l'égard des services souhaitant utiliser ses données personnelles. Elle serait incitée à une implication plus active par les perspectives de valorisation de ses données. Sur le modèle du droit de la propriété littéraire et artistique, les individus pourraient former des sociétés de gestion collective de leurs données personnelles, qui négocieraient avec les services souhaitant les utiliser et redistribueraient les bénéfices à leurs associés. Enfin, le droit de propriété serait d'avantage reconnu par les États tiers que le droit à la protection des données personnelles.

L'objection la plus souvent formulée contre cette reconnaissance n'est pas dirimante. Il n'est certainement pas souhaitable que l'individu, par l'exercice du droit d'aliénation attaché au droit de propriété, renonce à toute protection sur ses données personnelles. Mais on peut envisager des démembrements du droit de propriété, comme en matière de domanialité publique (les personnes publiques sont propriétaires du domaine public mais ne peuvent l'aliéner) ou de droit d'auteur (les titulaires du droit d'auteur peuvent céder leurs droits patrimoniaux mais pas leur droit moral[454]). L'individu ayant cédé ses données ou des droits d'utilisation de celles-ci conserverait sur elles des droits inaliénables, tels que le droit d'accès ou de rectification.

Ce sont deux autres raisons qui conduisent en réalité à écarter la reconnaissance d'un droit de propriété de l'individu sur ses données : l'inaptitude à atteindre les objectifs recherchés (a) et la fragilisation de toute la réglementation publique de l'utilisation des données personnelles (b).

(a) Le rééquilibrage de la relation entre les éditeurs de services numériques et les internautes, qui découlerait de la reconnaissance d'un tel droit de propriété, apparaît largement illusoire. Sauf pour des personnalités d'une particulière richesse ou notoriété, la valeur des données d'un seul individu est très limitée, de l'ordre de quelques centimes ou de quelques dizaines de centimes ; c'est le très grand nombre des données traitées qui confère leur valeur aux bases manipulées par les acteurs du numérique. Même si le prix des données de chaque individu est appelé à croître de manière considérable au cours des années à venir (jusqu'à quelques euros), la valeur de l'actif que la reconnaissance du droit de propriété conférerait à chaque individu restera dérisoire. Les acteurs du numérique rédigeraient leurs contrats comme la fourniture d'un service en échange de la cession de droits d'utilisation des données, ce dont nombre de conditions générales d'utilisation se rapprochent déjà beaucoup ; le rapport de forces entre l'individu, consommateur isolé et l'entreprise, resterait marqué par un déséquilibre structurel.

454. Défini par l'article L. 121-1 du code de la protection intellectuelle comme un droit perpétuel, inaliénable et imprescriptible.

La création de sociétés de gestion collective aurait vocation à corriger ce déséquilibre. Toutefois, le modèle de ces sociétés, qui requièrent des frais de gestion significatifs et rassemblent des acteurs à l'identité professionnelle et aux intérêts bien définis, apparaît difficilement transposable au traitement des données personnelles : le nombre d'individus à associer serait infiniment plus important ; aucune identité professionnelle ne les fédérerait ; les frais de gestion seraient lourds à supporter au regard du caractère minime des sommes à recouvrer et du coût de leur répartition entre une multitude d'ayant-droits.

Enfin, rien ne garantit qu'un droit de propriété de l'individu sur ses données institué de manière unilatérale par un État serait reconnu par les autres États. En matière de propriété immatérielle, chaque État définit les limites des droits qu'il reconnaît : ainsi, les droits moraux de l'auteur ne sont pas pleinement reconnus par les pays appliquant le système du *copyright*, qui ont une conception essentiellement patrimoniale du droit d'auteur. L'opposabilité du droit de propriété de l'individu à une entreprise traitant ses données personnelles et établie dans un État ne reconnaissant pas ce droit ne serait pas garantie ou se trouverait subordonnée à la signature d'accords internationaux.

(b) La reconnaissance du droit de propriété de l'individu sur ses données pourrait poser de sérieuses difficultés juridiques pour les pouvoirs publics. En effet, la législation actuelle énonce plusieurs limites à la capacité d'un individu de décider de l'utilisation de ses données : d'une part, certains traitements de données justifiés par un intérêt public peuvent lui être imposés ; d'autre part, son consentement ne dispense pas le responsable du traitement de respecter les principes définis par l'article 6 de la loi du 6 janvier 1978. Si un droit de propriété était reconnu, ces limites deviendraient des atteintes à l'exercice du droit de propriété, qui devraient dès lors être justifiées au regard de la jurisprudence de la CEDH et du Conseil constitutionnel. Selon la jurisprudence développée par la CEDH sur le fondement de l'article 1er du premier protocole additionnel à la Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales, les atteintes à l'exercice du droit de propriété doivent être justifiées par un but d'utilité publique, prévues par la loi et proportionnées. On peut estimer que la plupart des traitements imposés par la législation, tels que les fichiers de police ou des impôts, répondraient à ces conditions. En revanche, si l'individu avait la pleine propriété de ses données, il serait plus difficile au législateur de lui imposer des principes définis par l'article 6.

La reconnaissance d'un droit de propriété de l'individu impliquerait en réalité de renoncer largement à la logique de protection. Un de ses partisans, Me Alain Bensoussan, l'admet d'ailleurs puisqu'il écrit : « *Il faut d'abord reconnaître des droits, par la propriété des données, et dans un second temps accorder une protection par exception, si c'est nécessaire. (…) La liberté de décision doit être le principe fondamental et la protection, l'exception* »[455]. L'objet même du droit de propriété est de permettre aux personnes de disposer librement de leurs biens. Sauf à l'entourer de tant de restrictions qu'il ne serait plus un droit de propriété, il ne peut être porteur des mêmes restrictions objectives à l'utilisation des données par les tiers que le droit actuel.

455. Cité dans CNIL, op. cit, p. 47.

Somme toute, la reconnaissance du droit de propriété impliquerait une moindre capacité de protection des pouvoirs publics sans renforcer pour autant la capacité des individus à veiller à leurs propres intérêts. Reste le paradoxe d'une appropriation généralisée qui n'échappe qu'à la personne concernée, mais ce paradoxe n'est qu'apparent : le droit de la propriété intellectuelle protège l'investissement dans la constitution de la base de données, non la donnée brute. Face aux droits des investisseurs en bases de données que sont les acteurs du numérique, l'individu a des droits à faire valoir, mais ils sont d'une autre nature.

Envisager la protection des données personnelles comme un droit à l'autodétermination

Le droit à l'autodétermination informationnelle (« *Informationnelle Selbstbestimmung* ») a été proclamé par la Cour constitutionnelle fédérale de l'Allemagne dans un arrêt du 15 décembre 1983, relatif à une loi sur le recensement. La Cour le déduit des articles 1er (dignité de l'homme) et 2 (droit au libre développement de sa personnalité) de la Loi fondamentale ; elle juge que « *la Constitution garantit en principe la capacité de l'individu à décider de la communication et de l'utilisation de ses données à caractère personnel* »[456]. Le droit à l'autodétermination informationnelle irrigue la jurisprudence postérieure de la Cour en matière de protection des données personnelles, concernant par exemple la recherche policière par recoupements dans le cadre de la lutte contre le terrorisme ou la collecte de données dans le cadre des assurances[457].

Cette notion propre au droit allemand n'a jamais été reprise à ce jour par des textes européens ou internationaux. Elle est pourtant de nature à renouveler le sens de la protection des données à caractère personnel. Quatre avantages sont à en attendre.

Tout d'abord, le fait que la Charte des droits fondamentaux de l'Union européenne ait érigé le droit à la protection des données en droit distinct présente l'inconvénient de laisser penser qu'il s'agit d'un but en soi, qui se suffit à lui-même. Le droit à l'autodétermination informationnelle lui donne un sens : il s'agit de donner à l'individu les moyens de demeurer libre de conduire son existence, dans une société où le numérique prend une place croissante, qui l'amène à laisser, de plus en plus souvent, trace de ses données personnelles. Selon les termes de la Cour de Karlsruhe, « *si l'individu ne sait pas prévoir avec suffisamment de certitude quelles informations le concernant sont connues du milieu social et à qui celles-ci pourraient être communiquées, sa liberté de faire des projets ou de décider sans être soumis à aucune pression est fortement limitée* ».

En deuxième lieu, alors que le droit à la protection des données peut-être perçu comme un concept défensif, le droit à l'autodétermination lui donne un contenu

456. Traduction en français de Y. Poullet et A. Rouvroy, « Le droit à l'autodétermination informationnelle et la valeur du développement personnel. Une réévaluation de l'importance de la vie privée pour la démocratie. », in *État de droit et virtualité,* K. Benyekhlef & P. Trudel (dir.). Montréal : Thémis, 2009.

457. BVerfG, 1 BvR 518/02, 4 avril 2006 ; BVerfG, 1 BvR 2027/02, 23 octobre 2006.

positif. Il ne s'agit plus seulement de protéger le droit au respect de la vie privée mais d'affirmer la primauté de la personne qui doit être en mesure d'exercer sa liberté. En ce sens, le droit à l'autodétermination répond d'avantage à l'aspiration croissante des individus à l'autonomie de décision. C'est cette aspiration que la proposition de droit de propriété sur les données essaie de saisir ; le droit à l'autodétermination y apporte une réponse à la fois plus efficace et plus conforme à la logique personnaliste et non patrimoniale qui a toujours prévalu en Europe en matière de protection des données. Là où le droit de propriété prétend faire des individus des gestionnaires d'un patrimoine, le droit à l'autodétermination rappelle qu'ils doivent demeurer en mesure de décider de leur existence. L'un se situe sur le plan de l'avoir, l'autre sur celui de l'être.

En troisième lieu, le droit à l'autodétermination informationnelle permet de prendre la mesure des enjeux pour les libertés publiques de la protection des données personnelles. Comme l'écrit la Cour, si l'individu « *craint que la participation à une assemblée ou à une initiative des citoyens soit officiellement enregistrée et qu'il coure personnellement des risques en raison de cette participation, il renoncera probablement à l'exercice de ses droits* » et « *ceci n'a pas seulement un impact sur ses chances de se développer, le bien-être commun en est aussi affecté car l'autodétermination est une condition élémentaire fonctionnelle dans une société démocratique libre, basée sur la capacité des citoyens d'agir et de coopérer* ». En d'autres termes, le droit à la protection des données ne protège pas seulement les individus, mais aussi la société dans son caractère démocratique. La Cour reconnaît dans la même décision que des limites peuvent être imposées au droit à l'autodétermination informationnelle au nom de l'intérêt public. Prolongement numérique du droit au libre développement de sa personnalité prévu par l'article 2 de la Loi fondamentale allemande, le droit à l'autodétermination informationnelle est, comme lui, limité par la nécessité de ne pas violer les droits d'autrui, l'ordre constitutionnel ou la loi morale. Si je montre mes données génétiques à un futur employeur dans l'espoir d'être recruté, alors les autres candidats seront-ils, peut-être, tenus eux aussi de dévoiler ces informations. Le droit à l'autodétermination est plus apte que le droit de propriété à prendre en compte ces interdépendances et à intégrer les limites qu'elles imposent.

Enfin, tel qu'il est formulé par la Cour de Karlsruhe (« *la capacité de l'individu à décider de la communication et de l'utilisation de ses données à caractère personnel* »), le droit à l'autodétermination informationnelle apparaît d'une grande ambition, au regard de la perte générale de maîtrise par les individus de leurs données précédemment décrite (cf. *supra* 2.1.1). Certes, la seule affirmation de ce droit ne permet pas de le rendre effectif et les instruments de la protection des données doivent être profondément transformés pour y parvenir. Mais le droit à l'autodétermination informationnelle constitue l'objectif permettant d'offrir une véritable protection des données personnelles. Par son haut niveau d'exigence, le droit à l'autodétermination peut jouer un rôle d'aiguillon, tant pour les pouvoirs publics que pour les individus.

Le droit à l'autodétermination informationnelle a vocation à bénéficier également aux mineurs : souvent les premiers à diffuser sur internet les données personnelles qui les concernent, les mineurs sont particulièrement vulnérables. Le droit à la vie privée, dans lequel s'enracine le droit à l'autodétermination informationnelle, leur est expressément reconnu par la convention internationale des droits de l'enfant[458]. Toutefois, compte tenu de la vulnérabilité des mineurs et de leur incapacité juridique, ce droit doit s'exercer dans le respect des prérogatives des parents[459]. Si la loi du 6 janvier 1978 ne comporte aucune disposition spécifique pour les mineurs, la doctrine constante de la CNIL requiert le consentement des parents pour la collecte de données personnelles les concernant. Le projet de règlement de l'Union européenne impose de recueillir un consentement vérifiable des parents pour la collecte des données de mineurs de moins de 13 ans.

Il n'apparaît pas souhaitable d'ajouter le droit à l'autodétermination à la liste des droits déjà reconnus par les textes existants ou que la proposition de règlement de l'Union européenne envisage de reconnaître, tels que les droits d'information, d'accès, de rectification ou d'opposition. Le droit à l'autodétermination se situe à un autre niveau : il donne sens à tous ces droits, qui tendent à le garantir et doivent être interprétés et mis en œuvre à la lumière de cette finalité. Il pourrait donc être inscrit dans les considérants de la proposition de règlement ou dans un article introductif, qui prévoirait que les individus jouissent du droit à l'autodétermination informationnelle, c'est-à-dire du droit de décider de la communication et de l'utilisation de leurs données à caractère personnel, dans les conditions et limites définis par le règlement. Sans attendre l'adoption du règlement, cette même formule pourrait être inscrite dans la loi du 6 janvier 1978.

Proposition n° 1 : Concevoir le droit à la protection des données personnelles comme un droit à « l'autodétermination informationnelle », c'est-à-dire le droit de l'individu de décider de la communication et de l'utilisation de ses données à caractère personnel.

Inscrire cette conception dans la proposition de règlement relatif à la protection des données à caractère personnel ou, dans l'attente du règlement, dans la loi du 6 janvier 1978.

Ne pas faire entrer les données personnelles dans le champ du droit de propriété patrimonial des personnes.

Vecteur : règlement de l'Union européenne ou loi.

458. Article 16.1 : « *Nul enfant ne fera l'objet d'immixtions arbitraires ou illégales dans sa vie privée, sa famille, son domicile ou sa correspondance, ni d'atteintes illégales à son honneur et à sa réputation.* ».

459. Sur les conditions d'exercice du droit à la protection des données personnelles des mineurs, cf. CNIL, *Internet et la collecte de données personnelles auprès des mineurs*, janvier 2001 ; Article 29 Working Party, *Opinion 2/2009 on the protection of children's personal data*, février 2009, 398/09/EN WP 160 ; Défenseur des droits, *Enfants et écrans : grandir dans le monde numérique*, rapport 2012 consacré aux droits de l'enfant.

3.1.2. Neutralité des réseaux, loyauté des plateformes

Deux catégories d'acteurs jouent un rôle particulièrement important dans la diffusion des contenus sur internet : les opérateurs de communications électroniques, qui les acheminent jusqu'aux utilisateurs finaux ; les plateformes, qui proposent des services de référencement et de classement indispensables pour faire le tri dans la masse des informations et des services disponibles. Ces rôles en font des intermédiaires obligés dans l'exercice de la liberté de communication, de la liberté d'entreprendre et de la liberté d'association sur internet ; ils leur créent donc des obligations. Ces obligations ne sont cependant pas de même nature : les opérateurs de communications électroniques doivent respecter un principe de neutralité, assorti de certaines dérogations ; les plateformes, qui ne sauraient être neutres puisque leur rôle est de classer, doivent être loyales envers leurs utilisateurs.

Consacrer le principe de neutralité des réseaux

Le principe selon lequel les opérateurs doivent traiter de manière égale l'ensemble du trafic qu'ils acheminent est bon. Il permet à chaque utilisateur d'accéder aux contenus de son choix dans les mêmes conditions et, réciproquement, à chaque fournisseur de contenus d'accéder à tous les utilisateurs dans les mêmes conditions. Il est ainsi une garantie de la liberté de communication, de la liberté d'entreprendre et de la liberté d'association, ce qui justifie qu'il soit protégé par la loi.

La consécration du principe de neutralité des réseaux apparaît particulièrement nécessaire aujourd'hui. La part du trafic représentée par les flux de vidéo diffusés par quelques sites et la puissance de marché acquise par leurs éditeurs rendent crédible le scénario d'un accaparement de la bande passante et de la qualité de diffusion par quelques acteurs dominants. Plusieurs grands États ont inscrit dans le droit positif leurs choix en matière de neutralité du *net* : le Brésil vient d'adopter une conception stricte de ce principe ; aux États-Unis, la *Federal Communications Commission* (FCC) soumet à concertation une nouvelle version plus souple de ses règles d'ouverture d'internet (« *Open Internet Rules* ») après l'annulation des règles de 2010 par une cour d'appel fédérale[460]. L'Union européenne doit à son tour adopter sa propre conception dans le cadre de la proposition de règlement établissant des mesures relatives au marché unique européen des communications électroniques et visant à faire de l'Europe un continent connecté.

Tout comme le principe d'égalité, qui admet des différences de traitement lorsqu'elles sont justifiées par des différences de situation ou par un motif d'intérêt général, le principe de neutralité du *net* doit laisser aux opérateurs de communications des espaces de différenciation. Comme il a été exposé ci-dessus (cf. 2.2.1), le projet de règlement dans sa rédaction votée par le Parlement européen le 3 avril 2014, apparaît excessivement restrictif. L'étude du Conseil d'État, tout en retenant la définition du principe de neutralité du *net* introduite par le Parlement européen estime que trois corrections devraient lui être apportées.

- La définition des mesures de gestion de trafic, qui ne seraient autorisées que pour faire face à une congestion « *temporaire et exceptionnelle* », est trop restrictive. Il

460. *Verizon vs FCC*, 14/1/2014, n° 11-1355.

convient de revenir sur ce point à la rédaction de la Commission, qui autorisait de telles mesures pour faire face à une congestion « *temporaire ou exceptionnelle* ».

- La définition des « *services spécialisés* » (ou « *services gérés* »), réservée aux services « *offrant une fonctionnalité nécessitant une qualité supérieure de bout en bout* », est elle aussi trop restrictive : il serait souhaitable que des services de qualité supérieure se développent même si un tel degré d'exigence n'est pas strictement nécessaire au service. Le choix d'une définition plus large doit en revanche s'accompagner de garanties plus fermes de l'absence de dégradation de la qualité générale d'internet. Les accords conclus entre les fournisseurs de contenus et d'applications et les opérateurs de communications électroniques tendant à garantir une qualité de service supérieure pour des services spécialisés devraient être notifiés préalablement à l'autorité de régulation compétente ; celle-ci aurait le pouvoir de s'y opposer en cas de risque manifeste de dégradation de la qualité générale d'internet en-deçà d'un niveau satisfaisant. L'autorité de régulation effectuerait également, *a posteriori*, un contrôle en continu de la qualité de l'accès à internet et aurait le droit de suspendre l'accord en cas de dégradation.

- Il n'apparaît pas souhaitable que les opérateurs de communications électroniques puissent, de manière générale, facturer aux fournisseurs de contenus l'accès aux utilisateurs finaux ; une facturation généralisée risquerait d'évincer les fournisseurs de contenus les plus petits et donc de nuire à la liberté de communication et à la liberté d'entreprendre. En revanche, il serait envisageable d'instaurer une facturation asymétrique, qui ne s'appliquerait qu'aux plus gros fournisseurs de contenus, représentant à eux seuls une part significative du trafic. Ces gros fournisseurs devraient alors payer, non pour bénéficier d'une qualité supérieure, mais pour ne pas voir leur qualité d'accès dégradée[461]. La mise en place d'une telle facturation asymétrique permettrait de satisfaire à la demande de rééquilibrage des relations avec les gros fournisseurs de contenus formulée par les fournisseurs d'accès internet, sans porter atteinte à la liberté de communication des acteurs de petite et moyenne taille. Comme pour la proposition n° 2, on peut anticiper l'adoption du règlement en inscrivant le principe de neutralité dans la loi du 6 janvier 1978.

Enfin, il convient de souligner que si le principe de neutralité, tel qu'il est formulé par la proposition de règlement, s'impose aux opérateurs de communications électroniques mais pas aux fournisseurs de contenus, ceux-ci ne sont pas exempts de toute obligation à l'égard des opérateurs. Comme tout acteur économique, ils sont tenus au respect d'un principe de non-discrimination et ne doivent pas pratiquer de différenciation injustifiée dans leur manière de traiter avec les différents opérateurs

461. Dans un cadre légèrement différent, puisqu'il s'agissait de la relation entre un fournisseur d'accès à internet (*Orange*) et un opérateur de transit (*Cogent*), l'Autorité de la concurrence a admis la facturation par le FAI de l'accès à ses utilisateurs finaux, au vu de la disproportion entre le trafic allant d'*Orange* vers *Cogent* et le trafic allant en sens inverse, environ 13 fois plus élevé (décision n° 12-D-18 du 20 septembre 2012) ; cette décision a été confirmée par la cour d'appel de Paris dans un arrêt du 19 décembre 2013 (n° 2012/19484). Le raisonnement peut être transposé à la relation entre un fournisseur d'accès à internet et un gros fournisseur de contenus, d'autant plus que dans cette affaire, la disproportion de trafic venait principalement de l'acheminement par *Cogent* du site de téléchargement *MegaUpload*.

de communications, par exemple en refusant l'interconnexion avec certains fournisseurs d'accès. Dans cet esprit, l'ordonnance n° 2011-1012 du 24 août 2011 a donné à l'ARCEP un pouvoir de règlement des différends qui met sur le même plan les opérateurs de communications et les fournisseurs de contenus[462]. La consécration par le règlement du principe de neutralité s'imposant aux opérateurs ne doit pas conduire à remettre en cause cette capacité du régulateur à traiter également les plaintes des opérateurs contre les fournisseurs de contenus.

Proposition n° 2 : Consacrer le principe de neutralité des opérateurs de communications électroniques dans les termes votés par le Parlement européen le 3 avril 2014, sous trois réserves :

- Revenir à la définition des mesures de gestion de trafic de la proposition de la Commission ;

- Revenir à la définition plus large des « services spécialisés », mais avec des contreparties : information préalable de l'autorité de régulation concernée sur le projet de convention ; droit d'opposition si risque manifeste de dégradation de la qualité de l'internet en-deçà d'un niveau satisfaisant ; droit de suspension de l'autorité de régulation s'il s'avère que qualité de l'internet est dégradée ;

- Droit des opérateurs d'exiger un paiement des fournisseurs de contenus, dans le cadre d'une facturation asymétrique, lorsqu'ils représentent à eux seuls une part significative du trafic.

Vecteur : loi ou règlement de l'Union européenne.

Définir la catégorie juridique des plateformes et les soumettre à une obligation de loyauté

La catégorie actuelle des hébergeurs, définis par leur rôle « *technique et passif* » et leur absence de connaissance et d'intervention sur les informations stockées, ne correspond plus à la réalité des plateformes, qui jouent un rôle actif de présentation, de référencement et de classement. Comme il a été vu ci-dessus (cf. 2.2.1), la Cour de cassation a écarté la qualification d'hébergeur pour la société *e-Bay* et le tribunal de grande instance de Paris a fait de même pour le service de recherche de *Google*. À moyen terme, tous les grands services d'intermédiation utilisés sur internet pourraient perdre la qualification d'hébergeur et le régime de responsabilité civile et pénale limitée qui en découle. La définition d'une nouvelle catégorie juridique est devenue nécessaire.

Le Conseil d'État propose la création d'une nouvelle catégorie de « *prestataires intermédiaires* » au sens de la directive n° 2000/31/CE du 8 juin 2000 sur le commerce électronique, distincte de celle des hébergeurs, intitulée « plateforme ». Seraient ainsi qualifiés les services de référencement ou de classement de contenus, biens

462. Selon le 5° de l'article L. 36-8 du CPCE, l'ARCEP peut être saisie des différends portant sur « *les conditions réciproques techniques et tarifaires d'acheminement du trafic entre un opérateur et une entreprise fournissant des services de communication au public en ligne* ».

ou services édités ou fournis par des tiers et partagés sur le site de la plateforme. Une telle définition couvrirait l'ensemble des acteurs usuellement considérés aujourd'hui comme des plateformes : moteurs de recherche, réseaux sociaux, sites de partage de contenus (vidéos, musique, photos, documents, etc.), places de marché, magasins d'applications, agrégateurs de contenus ou comparateurs de prix. Par son caractère générique, elle pourrait également couvrir à l'avenir de nouveaux types de services encore peu développés ou inexistants à l'heure actuelle. Cette définition cherche à capturer ce qui caractérise la plateforme, c'est-à-dire son rôle d'intermédiaire actif dans l'accès à des contenus, des biens ou des services qui ne sont pas produits par elle. C'est ce rôle d'intermédiaire qui justifie le maintien d'un régime de responsabilité limitée, qui sera présenté plus loin (cf. *infra* 3.3.3, proposition n° 28).

La catégorie des plateformes ici proposée ne couvre en revanche pas les acteurs ayant une responsabilité directe dans la production ou la sélection des contenus mis en ligne. Ainsi, les sites de musique en ligne[463] ou de vidéo à la demande[464], qui définissent entièrement le catalogue des œuvres mises en ligne et sont titulaires des droits de diffusion de celles-ci, ne sont pas des plateformes. Il en va de même, de manière générale, des distributeurs de services audiovisuels au sens de l'article 2-1 de la loi du 30 septembre 1986 relative à la liberté de communication : ceux-ci sont en effet définis comme une personne « *qui établit avec des éditeurs de services des relations contractuelles en vue de constituer une offre de services de communication audiovisuelle* » ; le distributeur procède donc au choix des contenus qu'il distribue en vue de constituer son offre de services.

Par ailleurs, une même entreprise peut être qualifiée de plateforme pour certaines de ses activités et d'éditeur ou de distributeur pour d'autres. Par exemple, un site de partage de contenus doit être qualifié de plateforme lorsque les contenus sont mis en ligne par des tiers sans sélection préalable, de distributeur lorsqu'il diffuse une chaîne de programmes dans le cadre d'un accord avec un éditeur, et d'éditeur s'il produit lui-même des contenus.

Les plateformes ne peuvent être soumises comme les opérateurs de communications électroniques à une obligation de neutralité. Leur liberté éditoriale, consistant à proposer le classement ou la présentation qui leur paraissent les plus pertinents, doit être respectée. En revanche, les plateformes doivent être tenues à une obligation de loyauté, tant à l'égard des utilisateurs finaux que des tiers qui mettent en ligne leurs contenus ou proposent leurs biens ou leurs services. La loyauté consiste à assurer de bonne foi le service de classement ou de référencement, sans chercher à l'altérer ou à le détourner à des fins étrangères à l'intérêt des utilisateurs. La plateforme doit avoir le choix des critères présidant à son classement ; mais ces critères doivent être pertinents par rapport à l'objectif de meilleur service rendu à l'utilisateur et ne peuvent par exemple être liés au fait que la plateforme favorise ses propres entités au détriment de services concurrents ou a passé des accords de partenariat dont l'utilisateur n'aurait pas connaissance. Le devoir général de loyauté se traduit en obligations multiples à

463. Tels que *Deezer* ou *Spotify*.
464. Tels que *Netflix* ou *FilmoTV*.

l'égard des utilisateurs commerciaux et non commerciaux (propositions n° 6 et n° 10) ; il vaut aussi en tant qu'obligation générale, dont le juge pourra découvrir toutes les implications au fil des litiges qui se présentent devant lui.

Il apparaît difficile de créer une telle catégorie de manière autonome dans la législation nationale. D'une part, elle ne serait pas compatible avec les termes actuels de la directive sur le commerce électronique. En effet, en définissant un régime de responsabilité et une obligation de loyauté des plateformes, la loi fixerait des règles relatives à « *l'exercice de l'activité d'un service de la société de l'information* » et entrerait donc dans le « *domaine coordonné* » au sens de l'article 2 h) de la directive, domaine à l'intérieur duquel les États ne peuvent fixer d'exigence non prévues par la directive. D'autre part, l'existence d'une catégorie juridique distincte dans la seule législation française poserait d'importantes difficultés pratiques. Une modification de la directive 2000/31 du 8 juin 2000 sur le commerce électronique devrait donc être recherchée. Les progrès de la jurisprudence, susceptibles de fragiliser toujours davantage la catégorie actuelle d'hébergeur, devraient y pousser.

Proposition n° 3 : Définir la catégorie juridique des plateformes, distincte de celle des simples hébergeurs passifs. Seraient qualifiés de plateformes les services de référencement ou de classement de contenus, biens ou services édités ou fournis par des tiers et partagés sur le site de la plateforme. Les plateformes seraient soumises à un principe de loyauté.

Vecteur *: directive de l'Union européenne.*

3.2. Renforcer les pouvoirs des individus et de leurs groupements

3.2.1. Renforcer les capacités d'action individuelle

Promouvoir le développement des technologies renforçant la maîtrise de la personne sur l'utilisation de ses données

Comme il a été vu ci-dessus (cf. 2.1.3), le champ des technologies renforçant la maîtrise de la personne sur l'utilisation de ses données est vaste. Il couvre notamment les outils de paramétrage du traçage des données personnelles par des *cookies* ou des dispositifs analogues, les outils de visualisation et de gestion des données personnelles détenues par des tiers, la standardisation des politiques d'utilisation des données par les fournisseurs de services numériques dans des formats lisibles par la machine ou encore l'apposition de métadonnées encadrant l'utilisation des données personnelles. Un constat doit toutefois être fait. Le développement de ces outils, qui demeure modeste, s'est jusqu'à présent réalisé

sans intervention notable des pouvoirs publics[465]. Ceux-ci pourraient encourager ce développement de manière plus active, afin de renforcer le pouvoir des citoyens sur l'utilisation de leurs données et de servir ainsi le droit à l'autodétermination informationnelle. Comme il a été indiqué dans la deuxième partie, cette mission couvrirait les technologies renforçant la maîtrise de la personne sur l'utilisation de ses données, mais pas les technologies de dissimulation des données, en raison des risques de ces dernières pour la protection de l'ordre public.

Le législateur pourrait confier ce rôle à la CNIL. Aux quatre missions aujourd'hui prévues par l'article 11 de la loi du 6 janvier 1978 (information des personnes concernées et des responsables de traitement sur leurs droits et obligations, contrôle de la conformité des traitements de données à la législation, corégulation avec les organisations professionnelles, veille sur l'évolution des technologies) s'ajouterait ainsi une cinquième mission, qui permettrait à la CNIL d'évaluer le potentiel des technologies de renforcement de la vie privée, d'analyser les obstacles à leur plus large diffusion, d'organiser des discussions entre les parties prenantes (éditeurs de logiciels, fournisseurs d'accès à internet, éditeurs de services numériques, représentants des consommateurs, etc.), voire de développer ou de faire développer elle-même de nouveaux outils, en veillant dans ce cas au respect du droit de la concurrence[466]. La même fonction pourrait être confiée par le législateur européen à l'ensemble des autorités nationales de protection des données.

Il reviendrait dès lors à ces régulateurs d'identifier les technologies les plus prometteuses et les instruments les plus propices à leur développement. Quelques pistes peuvent être avancées ici :

- Un dialogue avec les parties prenantes destiné à susciter l'émergence des solutions les plus prometteuses pourrait être organisé à l'échelle européenne, à l'exemple de l'exercice « *Licenses for Europe* » qui a été conduit par la Commission européenne en 2013 au sujet de la diffusion paneuropéenne des contenus culturels respectant le droit de propriété intellectuelle.

- Afin de favoriser la découverte et l'utilisation par le grand public des technologies de renforcement de la vie privée, les fournisseurs d'accès à internet pourraient offrir gratuitement à leurs clients de tels outils, soit par une politique incitative, soit en vertu d'une obligation légale analogue à celle qui leur impose de fournir des outils de contrôle parental (1. du I de l'article 6 de la LCEN).

- La standardisation des politiques d'utilisation des données personnelles des entreprises a été inscrite dans le projet de règlement européen, dans sa version votée par le Parlement européen le 12 mars 2014 (article 13 *bis*). Cette standardisation pourrait rééquilibrer de trois manières la relation entre les

465. Même si l'on peut signaler la fourniture gratuite au public par la CNIL d'un outil de visualisation des *cookies*, *Cookieviz*, en décembre 2013, et sa participation au projet *MesInfos* de la Fondation Internet Nouvelle Génération (FING).

466. CE, Ass., 31 mai 2006, *Ordre des avocats au barreau de Paris*, n° 275531, Rec. p. 272. : pour intervenir sur un marché, des personnes publiques doivent justifier d'un intérêt public et ne pas fausser le jeu de la concurrence par rapport aux autres opérateurs agissant sur le même marché.

internautes et les entreprises utilisant leurs données personnelles. Tout d'abord, les conditions d'utilisation des données deviendraient aisément compréhensibles par les internautes. Ensuite, les internautes pourraient adhérer à des règlements-type définissant des polices d'utilisation qui pourraient être établies par des associations de défense des consommateurs ou de la vie privée, encadrant l'utilisation des données personnelles. Enfin, ils pourraient paramétrer leurs navigateurs pour n'utiliser que les sites qui offrent un niveau de protection équivalent ou supérieur à celui de leur règlement type[467]. Si un nombre suffisant d'internautes suivait ce type de démarches, le rapport de forces avec les entreprises serait modifié : celles-ci ne pourraient plus définir unilatéralement leurs conditions d'utilisation mais seraient obligées de tenir compte des réglements-types les plus suivis. Si la disposition votée par le Parlement européen est définitivement adoptée, les autorités de protection telles que la CNIL pourraient susciter l'élaboration de polices d'utilisation, voir proposer leurs propres réglements types aux internautes.

- Enfin, l'intervention de prestataires « tiers de confiance », jouant un rôle d'intermédiation dans la relation entre la personne et les organismes traitant ses données personnelles, afin de garantir que ces organismes n'ont accès qu'aux données dont la personne a autorisé la divulgation, pourrait être développée. La CNIL pourrait définir à leur égard des recommandations de bonnes pratiques.

Proposition n° 4 : Donner à la CNIL et à l'ensemble des autorités de protection des données européennes une mission explicite de promotion des technologies renforçant la maîtrise des personnes sur l'utilisation de leurs données.

Envisager notamment les actions suivantes :

- Lancer au niveau européen une concertation multiacteurs dans le but de susciter l'émergence des solutions technologiques les plus prometteuses en termes de renforcement de la vie privée ;

- Promouvoir la diffusion gratuite d'outils de renforcement de la vie privée par les FAI, soit dans un cadre volontaire, soit en l'imposant par la loi comme c'est le cas pour les logiciels de contrôle parental ;

- Dans le cadre de la standardisation des politiques d'utilisation des données personnelles prévue par le projet de règlement européen, susciter le développement de règlements types définissant des polices d'utilisation, auxquels un grand nombre d'internautes adhéreraient et que les entreprises seraient donc conduites à prendre en compte pour définir leur propre politique.

- Développer l'intervention de prestataires « tiers de confiance », afin de garantir que seules les données dont la personne a autorisé la divulgation sont diffusées.

Vecteur *: Loi, règlement de l'Union européenne, action de la CNIL et des autres autorités européennes de protection des données.*

Mettre en œuvre de manière efficace le droit au déréférencement reconnu par la CJUE

L'arrêt *Google Spain* du 13 mai 2014 de la CJUE a ouvert la voie à un grand nombre de demandes de déréférencement émanant de particuliers. Il reviendra aux exploitants de moteurs de recherche de traiter ces demandes, sous le contrôle des autorités de protection des données et des juridictions nationales. Une certaine durée sera sans doute nécessaire pour que les implications de l'arrêt dans les différentes situations pratiques soient clarifiées, notamment grâce au développement de la jurisprudence. Dès à présent, et au vu des premières démarches mises en œuvre par les exploitants pour se conformer à l'arrêt[468], quatre actions apparaissent souhaitables :

- Toute demande de déréférencement met en cause au moins trois acteurs : le demandeur, l'exploitant du moteur de recherche, mais aussi l'éditeur du site dont le déréférencement est demandé. Les procédures définies par les exploitants doivent permettre à l'éditeur du site de faire valoir ses observations, notamment au sujet de l'intérêt du public à avoir accès à l'information et, le cas échéant, de saisir le juge, seul à même de procéder à la conciliation des libertés fondamentales et à un juste équilibre entre les droits et intérêts en présence.

- Il importe de préciser que le déréférencement doit concerner l'ensemble des versions « nationales »[469] d'un même moteur de recherche. En effet, l'applicabilité des obligations de déréférencement telles que les a énoncées la CJUE ne dépend que de la présence d'un établissement de l'exploitant du moteur de recherche dans un État membre de l'Union européenne ; le fait que le nom de domaine du site ait ou non une extension nationale d'un des États membres de l'Union est sans incidence. L'application du déréférencement par l'ensemble des versions d'un même moteur est nécessaire pour assurer l'effectivité de ce droit ; dans le cas contraire, il serait aisé pour un internaute de contourner le déréférencement en cherchant l'information sur une version « *non-européenne* » du site.

- Entre l'arrêt de la CJUE et les procédures mises en place par les exploitants de moteur de recherche, il y a place pour une intervention des pouvoirs publics explicitant les principes généraux de l'arrêt et aidant à leur mise en œuvre dans des cas particuliers. Ce rôle revient aux autorités nationales de protection des données, qui sont chargées, en vertu de la directive n° 95/46/CE de veiller à la mise en œuvre des droits d'opposition et d'effacement sur lesquels est fondé le droit au déréférencement. Les autorités de protection des données pourraient définir, par la voie de lignes directrices ayant le caractère d'instruments de droit souple,

467. Voir à ce sujet les propositions du conseil scientifique et technologique du président des États-Unis : President's Council of Advisors on Science and Technology (PCAST), *Big Data and Privacy : A Technological Perspective*, mai 2014, pp. 40-41.

468. La société *Google* a mis en ligne le 30 mai 2014 un formulaire de « *demande de suppression de résultat de recherche au titre de la législation européenne relative à la protection des données* » cf. https://support.google.com/legal/contact/lr_eudpa?product=websearch&hl=fr.

469. Dans le cas de *Google*, les versions nationales des pays européens (www.google.de, www.google.fr, www.google.it etc.), mais aussi www.google.com.

les orientations qui guideront leur décision lorsqu'elles se prononceront sur des recours formés par des particuliers. L'adoption de ces lignes directrices permettrait de répondre à l'argument selon lequel l'arrêt *Google Spain* conférerait aux moteurs de recherche un pouvoir discrétionnaire dans le choix des informations référencées. Leur portée serait sans doute plus grande si elles étaient adoptées de manière coordonnée au sein du G29.

- Si la part de marché de *Google* est très majoritaire en Europe, le droit au déréférencement concerne l'ensemble des moteurs de recherche. Dès lors qu'une demande de déréférencement est fondée au regard de l'arrêt *Google Spain*, il n'y a aucune raison pour qu'elle ne soit pas mise en œuvre par l'ensemble des exploitants[470]. Des particuliers pourraient être découragés de devoir adresser des demandes distinctes à chaque exploitant, dont les décisions risqueraient en outre d'être discordantes. Il serait donc souhaitable qu'une décision unique soit prise sur les demandes de déréférencement. Trois voies permettraient d'y parvenir : la reconnaissance mutuelle des décisions prises par chaque exploitant, sur la base d'un accord volontaire entre ceux-ci ; la création d'une instance commune de décision par les exploitants, qui mutualiseraient ainsi leurs charges ; la création par la loi de la possibilité d'étendre à tous les exploitants une décision de déréférencement prise par l'un d'entre eux, dès lors qu'elle serait homologuée par le juge, sur saisine du demandeur.

Proposition n° 5 : Mettre en œuvre de manière efficace et équilibrée le droit au déréférencement consacré par l'arrêt *Google Spain*, en :

- Donnant aux éditeurs des sites dont le déréférencement est demandé la possibilité de faire valoir leurs observations ;

- Explicitant par des lignes directrices la doctrine de mise en œuvre de *Google Spain* par les autorités de protection des données ;

- Organisant les conditions d'une décision unique de déréférencement, soit par accords de reconnaissance mutuelle des décisions de déréférencement prises par les exploitants de moteurs de recherche, soit par un dispositif légal d'extension à tous les exploitants d'une décision prise par l'un d'entre eux, sous réserve de son homologation par un juge.

Vecteur *: lignes directrices du G29 pour les deux premiers points ; accord entre les exploitants de moteurs de recherche ou loi pour le troisième.*

Définir les obligations des plateformes envers leurs utilisateurs, qui découlent du principe de loyauté

Le principe de loyauté des plateformes, énoncé ci-dessus (cf. 3.1.2, proposition n° 3), peut se décliner en une série d'obligations envers leurs utilisateurs non commerciaux et commerciaux. Il est ici proposé de définir quatre obligations :

470. Au sein de l'Union européenne, où *Google* dispose d'une part de marché supérieure à 90 %, les seuls autres moteurs représentant une part significative sont *Yahoo !* et *Bing*.

une obligation de pertinence des critères de classement et de référencement (a), d''information sur ces critères (b), un encadrement des retraits de contenus par la plateforme (c) et, en ce qui concerne les utilisateurs commerciaux, une obligation de notification préalable des changements d'algorithmes ou de politiques relatives aux contenus (d).

(a) Les plateformes sont libres, dans le cadre de leur liberté d'entreprendre, de définir les algorithmes de classement ou de référencement des contenus, produits ou services accessibles par leur intermédiaire, dans le but de fournir le service le plus efficace aux utilisateurs. Toutefois, le principe de loyauté leur interdit d'introduire dans ces algorithmes des considérations étrangères à l'intérêt des utilisateurs. Lorsque l'entreprise gestionnaire de la plateforme propose elle-même des services parmi ceux qu'elle référence, elle ne doit pas avantager ses propres services au détriment de ceux de ses concurrents ; cette question est l'un des principaux enjeux de la procédure en cours[471] devant la Commission européenne concernant *Google*. La plateforme ne doit pas non plus favoriser des services tiers avec lesquels elle aurait conclu des accords de partenariat ou introduire dans un classement en principe fondé sur des critères de pertinence pour l'utilisateur, des considérations liées à des sommes qu'elle aurait perçues pour avantager telle ou telle entité.

(b) Les algorithmes sont couverts par le secret industriel et la publication intégrale de leur code source ne serait de toute façon pas d'une grande aide pour la majorité des consommateurs. Toutefois, sans méconnaître le secret industriel, les plateformes devraient expliquer à leurs utilisateurs la logique générale de leurs algorithmes et, le cas échéant, la manière dont les utilisateurs peuvent les paramétrer. Lorsque la loi impose le retrait de contenus ou de sites internet vers lequel l'algorithme aurait conduit, ou impose la prise en compte par l'algorithme de certains critères, les utilisateurs doivent en être informés. Lorsque la plateforme introduit dans ses propositions une logique financière, liée aux sommes qui lui sont versées par des tiers pour être mis en avant, ou souhaite promouvoir ses propres services, ces propositions doivent être clairement distinguées de celles résultant de l'algorithme visant la pertinence pour l'utilisateur.

(c) Les plateformes retirent fréquemment des contenus mis en ligne sur leur site, soit en vertu de dispositions légales telles que l'article 6 de la LCEN, soit en vertu de leur propre politique de contenus. L'encadrement procédural et sur le fond de ces retraits devrait être renforcé :

- En termes de procédure, les droits de la personne ayant fait l'objet d'une telle mesure ne sont pas adéquatement protégés : le retrait lui est imposé sans qu'elle ait la possibilité de faire valoir ses observations et elle peut seulement entreprendre un recours juridictionnel. À cet égard, la législation américaine équivalente à la LCEN, le *Digital Millenium Copyright Act* (DMCA) de 1998, est plus respectueuse des droits de la personne faisant l'objet d'un retrait à la demande d'un ayant-droit : celle-ci dispose du droit de formuler une contre-notification contestant le caractère illicite du contenu retiré ; l'auteur de la demande dispose alors d'un délai

471. Au moment de la rédaction de la présente étude.

pour former un recours juridictionnel, à l'expiration duquel le contenu est rétabli. Cette possibilité de contre-notification, rarement utilisée, ne semble pas avoir nui particulièrement à l'efficacité de la lutte contre la contrefaçon aux États-Unis. Sans aller jusqu'à donner un tel pouvoir d'opposition à la personne faisant l'objet du retrait, celle-ci devrait avoir la possibilité de faire valoir ses observations et d'établir la licéité de son contenu ou sa conformité à la politique de la plateforme, selon le motif du retrait. Dès lors que selon le Conseil constitutionnel, la responsabilité de l'hébergeur (et demain de la plateforme si cette nouvelle catégorie juridique est créée) n'est engagée que si le contenu est manifestement illicite (décision n° 2004-496 DC du 10 juin 2004, *Loi pour la confiance dans l'économie numérique*, § 9), la plateforme ne serait plus tenue de retirer le contenu dès lors que la personne l'ayant déposé aurait produit des justifications convaincantes sur sa licéité.

- Sur le fond, des questions se posent quant aux retraits justifiés non par l'illicéité du contenu mais par sa non-conformité à la politique de la plateforme. Sur le principe, la possibilité pour une plateforme d'exclure certains contenus alors qu'ils sont autorisés par la loi n'est pas contestable : elle relève de sa liberté contractuelle et de sa liberté d'entreprendre[472]. Toutefois, les critères retenus doivent être clairement énoncés et accessibles à tous afin de ne pas laisser au gestionnaire de la plateforme une marge de décision arbitraire. Enfin, ils ne doivent pas être discriminatoires.

(d) L'équilibre économique des utilisateurs commerciaux des plateformes dépend souvent, de manière déterminante, de leur référencement et de leur classement. Cette considération a amené l'Autorité de la concurrence dans l'affaire *Navx c/ Google*, à accepter les engagements de la société *Google* visant à notifier, avec un délai de préavis de trois mois, les changements plus restrictifs de la politique de contenus de son service *AdWords*[473]. Dans l'esprit de cette décision, il pourrait être prévu de notifier aux utilisateurs commerciaux, avec un délai de réponse raisonnable, les changements de la politique de contenus et des changements d'algorithme susceptibles d'affecter leur référencement et leur classement. S'agissant des changements d'algorithme, la notification devrait comporter, dans la mesure où cela est techniquement réalisable, une estimation de l'incidence sur le classement de l'utilisateur concerné.

---

472. Selon les termes employés par l'Autorité de la concurrence dans sa décision n° 10-MC-01 du 30 juin 2010 relative à la demande de mesures conservatoires présentée par la société *Navx* (affaire *Navx c/ Google*) : « (…) *l'Autorité de la concurrence estime utile de souligner que la position dominante que Google est susceptible d'occuper sur le marché de la publicité en ligne liée aux recherches n'implique pas à elle seule (…) une obligation pour Google d'ouvrir son service AdWords à toute activité au seul motif que celle-ci ne serait pas interdite par les lois et règlements du pays dans lequel s'exerce cette activité. À titre d'illustration, il ressort de la libre appréciation de Google d'interdire en fonction de considérations objectives, comme elle le fait actuellement, les publicités pour les cigares, les stéroïdes anabolisants ou encore les feux d'artifices* ».

473. Décision n° 10-D-30 du 28 octobre 2010 relative à des pratiques mises en œuvre dans le secteur de la publicité sur Internet.

On peut envisager deux solutions pour mettre en œuvre ces droits. La première ferait une large utilisation du droit souple et n'aurait recours à la loi que pour énoncer le principe de loyauté et renvoyer la définition de ses implications à des chartes d'engagements professionnels élaborées par les plateformes. La seconde fixerait par la loi l'ensemble des droits présentés ci-dessus. Dans les deux cas, une telle loi devrait cependant être autorisée par une modification de la directive n° 2000/31/CE du 8 juin 2000 sur le commerce électronique, car elle toucherait aux conditions d'exercice de l'activité des plateformes.

Le contrôle et la sanction des manquements à l'obligation de loyauté relèveraient de différentes autorités, en raison de la diversité des utilisateurs des plateformes. Lorsque ces manquements affectent les consommateurs, ils pourraient être appréhendés et punis par la direction générale de la concurrence, de la consommation et de la répression des fraudes (DGCCRF), dont les pouvoirs ont été renforcés par la loi du 17 mars 2014 relative à la consommation. Lorsqu'ils concernent des professionnels utilisateurs de la plateforme, ils sont susceptibles d'entrer dans les compétences de l'Autorité de la concurrence, s'ils sont constitutifs d'abus de position dominante, ou dans celles de l'ARCEP, s'ils sont relatifs à un différend avec un FAI sur des conditions techniques et tarifaires d'interconnexion revêtant un caractère discriminatoire ou manquant de transparence. Enfin, le juge judiciaire pourrait toujours être saisi sur le terrain de la responsabilité ou dans le cadre des actions juridictionnelles spécifiques prévues par le droit de la consommation.

Proposition n° 6 : Définir les obligations des plateformes envers leurs utilisateurs, découlant du principe de loyauté :

- pertinence des critères de classement et de référencement mis en œuvre par la plateforme au regard de l'objectif de meilleur service rendu à l'utilisateur ;
- information sur les critères de classement et de référencement ;
- définition des critères de retrait de contenus licites en termes clairs, accessibles à tous, et non discriminatoires ;
- mettre l'utilisateur ayant mis en ligne un contenu en mesure de faire valoir ses observations en cas de retrait de celui-ci ;
- en ce qui concerne les utilisateurs commerciaux, notification préalable, avec un délai de réponse raisonnable, des changements de la politique de contenus ou de l'algorithme susceptibles d'affecter le référencement ou le classement.

Vecteur *: directive de l'Union européenne ou droit souple (chartes d'engagements des plateformes)*

Organiser un droit d'alerte en matière de protection des données personnelles

Les manquements à la législation relative à la protection des données personnelles ne sont pas toujours aisés à déceler. Dans un litige comme celui opposant *Google* à plusieurs autorités européennes de protection des données, c'est la politique officielle de confidentialité de l'entreprise qui est en cause ; mais dans de nombreux cas, les traitements effectivement réalisés peuvent ne pas correspondre à ceux qui ont été déclarés. De tels traitements peuvent être difficiles à appréhender, même dans le cadre d'un contrôle. C'est pourquoi l'ouverture d'un droit d'alerte aux salariés des entreprises et des organismes traitant des données personnelles, assurant une protection à ceux qui signalent de bonne foi des pratiques qu'ils estiment contraires à la législation, paraît utile pour compléter les moyens d'investigation des pouvoirs publics.

Le cadre législatif du droit d'alerte a connu ces dernières années en France un profond renouvellement. Des droits d'alerte spécifiques ont été créés en matière de lutte contre les discriminations[474], le harcèlement moral[475], le harcèlement sexuel[476], la corruption[477], les atteintes à la sécurité sanitaire des produits de santé[478], les risques graves pour la santé publique et l'environnement[479] et enfin les conflits d'intérêt[480]. En outre, à l'occasion de l'examen de la loi du 6 décembre 2013 relative à la lutte contre la fraude fiscale et la grande délinquance économique et financière, le Parlement a instauré un droit d'alerte général, qui garantit une protection aux salariés du secteur privé ou public lorsqu'ils relatent ou témoignent, de bonne foi, de faits constitutifs d'un délit ou d'un crime dont ils ont eu connaissance dans l'exercice de leurs fonctions[481].

Il existe dès lors deux bases légales possibles pour organiser un droit d'alerte en matière de protection des données personnelles :

- Ce droit d'alerte pourrait se fonder sur le droit d'alerte général issu de la loi du 6 décembre 2013. En effet, la plupart des manquements à la législation sur les données personnelles font l'objet en France d'incriminations pénales prévues par les articles 226-16 à 226-24 du code pénal, notamment le fait de procéder à

474. Article L. 1132-3 du code du travail.
475. Article L. 1152-2 du code du travail.
476. Article L. 1153-3 du code du travail.
477. Article L. 1161-1 du code du travail, issu de la loi n° 2007-1598 du 13 novembre 2007 relative à la lutte contre la corruption.
478. Article L. 5312-4-2 du code de la santé publique, issu de la loi n° 2011-2012 du 29 décembre 2011 relative au renforcement de la sécurité sanitaire du médicament et des produits de santé.
479. Article L. 5312-4-2 du code de la santé publique, issu de la loi n° 2011-2012 du 29 décembre 2011 relative au renforcement de la sécurité sanitaire du médicament et des produits de santé.
480. Article 25 de la loi n° 2013-907 du 11 octobre 2013 relative à la transparence de la vie publique.
481. Article L. 1132-3-3 du code du travail et article 6 ter A de la loi n° 83-634 du 13 juillet 1983 portant droits et obligations des fonctionnaires.

un traitement sans respecter les formalités préalables à sa mise en œuvre ou de collecter des données par un moyen frauduleux, déloyal ou illicite. La CNIL aurait seulement à indiquer que le droit d'alerte peut être exercé, dans un premier temps devant le correspondant informatique et libertés (CIL) de l'organisme lorsque celui-ci en est doté, puis devant elle, pour les infractions à la législation sur les données personnelles (les dispositions issues de la loi du 6 décembre 2013 ne précisent pas auprès de quelle autorité le droit d'alerte doit être exercé). Elle aurait également à mettre en place un mécanisme de signalement (par exemple sur une page dédiée de son site *web*) et à présenter aux salariés les garanties dont ils bénéficient en vertu de la loi du 6 décembre 2013.

- Un nouveau droit d'alerte spécifique pourrait être instauré par le législateur. Ce droit pourrait alors couvrir l'ensemble des manquements à la législation sur les données personnelles, y compris ceux qui ne font pas l'objet d'une incrimination pénale. Il pourrait s'exercer devant le correspondant informatique et libertés de l'entreprise, concomitamment ou préalablement à la saisine de la CNIL.

Compte tenu du grand nombre de droits d'alerte spécifiques créés au cours des dernières années, la première voie est préférable. Une communication active de la CNIL est préconisée pour faire connaître ce nouveau droit.

Proposition n° 7 : Mettre en œuvre le droit d'alerte pour les salariés des organismes traitant des données personnelles, par des processus d'information et de déclaration placés sous la responsabilité de la CNIL.

Vecteur *: action de la CNIL.*

3.2.2. Renforcer les capacités d'action collective

Créer une action collective en matière de protection des données personnelles

Les personnes affectées par une méconnaissance de la législation sur les données personnelles sont peu enclines à saisir la justice. L'enjeu pour chaque personne est en règle générale limité et le préjudice difficile à évaluer. En revanche, l'enjeu collectif peut être très important, par exemple dans le cas d'une faille de la sécurité ou d'une cession non autorisée de données personnelles affectant des centaines de milliers voire des millions de personnes. C'est pour apporter une réponse à ce type de situation, dans lequel une multitude de personnes sont concernées par un litige de faible enjeu pour chacune, que la loi du 17 mars 2014 relative à la consommation a créé la procédure d'action de groupe.

En l'état, cette procédure ne peut cependant s'appliquer que de manière limitée aux litiges ayant pour objet la protection des données personnelles. L'action de groupe ne peut viser que la réparation de « *préjudices patrimoniaux résultant des dommages matériels subis par les consommateurs* ». Or, les préjudices liés à la

méconnaissance de la législation sur les données personnelles peuvent rarement être ainsi qualifiés : il s'agit plus souvent de préjudices moraux liés à l'atteinte à la vie privée. En outre, les personnes ayant été lésées par l'utilisation de leurs données personnelles ne sont pas toujours des consommateurs, dès lors qu'il n'existe pas nécessairement de relation contractuelle commerciale entre eux et le responsable du traitement de leurs données : il en va par exemple ainsi lorsque les données sont collectées par un *data broker* ou par une régie publicitaire travaillant pour un site visité par l'internaute.

On pourrait penser à assouplir les conditions de l'action de groupe dans le domaine de la protection des données personnelles, en l'étendant aux préjudices moraux ainsi qu'aux personnes n'ayant pas la qualité de consommateur à l'égard de l'acteur qui a utilisé leurs données personnelles. Cette voie risquerait cependant de se heurter à la difficile évaluation des préjudices moraux liés à l'utilisation des données personnelles ; c'est d'ailleurs cette difficulté qui a conduit le Parlement à restreindre l'action de groupe aux préjudices patrimoniaux dans la loi du 17 mars 2014.

Il parait donc plus pertinent de créer une voie d'action spécifique, qui serait qualifiée d'action collective[482] pour la distinguer de l'action de groupe, dont l'objet serait de faire cesser la violation de la législation sur les données personnelles et non de réparer les préjudices individuels qu'elle a causés. La loi devrait définir les personnes habilitées à exercer cette action collective, la juridiction compétente et les prérogatives de celle-ci :

- Compte tenu de son objet collectif, l'action collective devrait être réservée à des groupements pouvant se prévaloir d'une représentativité reconnue par la loi : les associations de consommateurs agréées dans les conditions définies à l'article L. 411-1 du code de la consommation ; des associations ayant pour objet la protection de la vie privée et des données personnelles, pour lesquelles il serait instauré un agrément *ad hoc* délivré par l'État. Les organisations syndicales seraient également compétentes s'agissant des traitements de données des salariés mis en œuvre par les employeurs[483].

---

482. Pour la distinction entre action collective et action de groupe, cf. le rapport de la conseillère à la Cour de cassation Laurence Pécaut-Rivolier, *Lutter contre les discriminations au travail : un défi collectif*, décembre 2013. L'objet de l'action collective préconisée par ce rapport est de faire cesser la discrimination et non, comme dans une action de groupe, de réparer les préjudices individuels causés par celle-ci.

483. L'article L. 2313-2 du code du travail, en vertu duquel les délégués du personnel peuvent saisir en référé le conseil des prud'hommes pour faire cesser les atteintes aux droits des personnes, à leur santé physique et mentale ou aux libertés individuelles dans l'entreprise, permet d'ores et déjà d'obtenir du juge une injonction du juge tendant à mettre fin à un traitement de données personnelles illicite (Soc., 17 juin 2009, *Société Sanofi Chimie*, 08-40.274). Toutefois, le rapport de Laurence Pécaut-Rivolier a constaté que cette procédure était très peu mise en œuvre et qu'elle était peu adaptée à la lutte contre les atteintes collectives aux libertés. Il apparaît donc utile d'ouvrir également aux syndicats l'action collective qu'il est proposé ici de créer.

- L'action collective serait exercée devant le tribunal de grande instance, qui est la juridiction judiciaire de droit commun, à l'encontre du responsable du traitement des données. La juridiction judiciaire ne pourrait être compétente à l'égard des traitements mis en œuvre par les personnes publiques dans le cadre de missions de service public administratif. S'agissant de ces traitements, les recours existants devant la juridiction administrative permettent déjà de faire cesser les atteintes à la législation[484].

- Le tribunal de grande instance, lorsqu'il constate l'existence d'une violation de la législation, serait compétent pour enjoindre au responsable de traitement d'y remédier dans le délai qu'il fixe, le cas échéant sous astreinte.

Proposition n° 8 : Créer une action collective, distincte de l'action de groupe, destinée à faire cesser les violations de la législation sur les données personnelles. Cette action serait exercée devant le tribunal de grande instance par les associations agréées de protection de consommateurs ou de défense de la vie privée et des données personnelles.

Vecteur *: loi.*

Mettre en « Open Data *» toutes les déclarations et autorisations de traitements de données*

L'article 31 de la loi du 6 janvier 1978 dispose que la CNIL met à la disposition du public la liste des traitements ayant fait l'objet d'une déclaration ou d'une autorisation[485]. Sans doute en raison du très grand nombre de traitements concernés, cette liste, parfois dénommée « *fichier des fichiers* », n'est pas rendue publique. Les personnes intéressées peuvent seulement demander à la CNIL d'accéder à cette liste pour obtenir des informations sur un fichier déclaré ou autorisé, ce qui implique qu'ils aient déjà connaissance de l'existence de ce fichier.

La publication en *Open Data* de toutes ces informations (sous réserve des restrictions au droit de communication des documents administratifs prévues par l'article 6 de la loi du 17 juillet 1978[486]) serait d'un grand intérêt. Elle permettrait d'obtenir une vision complète, sinon de l'ensemble des traitements de données mis en œuvre en France, du moins de ceux dont la CNIL a connaissance. Le volume probablement très important de la base ne serait pas un obstacle, les outils du *Big Data* permettant aujourd'hui d'y faire face aisément et d'en extraire des statistiques pertinentes. Il serait par exemple possible d'identifier les secteurs d'activité les plus consommateurs de données, ou de détecter des zones blanches où le nombre de déclarations

484. Soit par la voie du référé-liberté, soit par celle d'un recours pour excès de pouvoir contre le refus de mettre fin à un traitement illicite, assorti le cas échéant de demandes d'injonction.
485. Accompagnée des informations que cet article énumère : acte décidant du traitement, dénomination et finalité, responsable du traitement, catégories de données traitées, etc.
486. Notamment les documents dont la communication porterait atteinte au droit à la vie privée ou au secret en matière commerciale ou industrielle.

apparaît peu important, ce qui peut suggérer l'existence d'une sous-déclaration. On peut noter que la CADA a pris en avril 2014 une décision comparable, en mettant en ligne l'ensemble de ses avis. Compte tenu de la charge administrative liée à la mise en ligne de la liste des traitements, celle-ci pourrait être progressive.

Le projet de règlement européen, en supprimant les déclarations de traitement, ferait disparaître une grande partie de ces informations. Pour y remédier, il devrait être envisagé d'imposer aux délégués à la protection des données, dont l'existence deviendra obligatoire dans de nombreuses entités, de publier chaque année un rapport d'information sur les traitements mis en œuvre dans leur organisme. Ces rapports seraient regroupés sur le site internet de l'autorité de protection des données et leur contenu standardisé, afin d'en faciliter l'exploitation statistique.

Proposition n° 9 : Mettre en *Open Data* toutes les déclarations et autorisations de traitements de données.

Vecteur *: action de la CNIL.*

Dans le cadre du projet de règlement européen, prévoir la publication sur le site de l'autorité de protection des données par les délégués à la protection des données, d'un rapport d'information annuel sur les traitements mis en œuvre par leur organisme.

Vecteur *: règlement de l'Union européenne.*

Promouvoir la concertation sur les règles éditoriales des plateformes

Comme il a été vu ci-dessus (cf. 2.3.1), les grandes plateformes (réseaux sociaux, sites de classement et de référencement de vidéos, magasins d'applications...) définissent des politiques éditoriales relatives aux contenus pouvant être mis en ligne sur leur site. Sur le principe, la définition de telles règles est légitime et relève de la liberté contractuelle et de la liberté d'entreprendre des plateformes. Toutefois, ces polices d'utilisation, qui ont le caractère de contrats-types proposés aux utilisateurs et relèvent ainsi du droit souple, jouent de fait un rôle considérable dans la définition des limites de la liberté d'expression sur internet. Certaines plateformes jouent un rôle tellement central que l'argument selon lequel un internaute mécontent de leurs règles peut toujours choisir de ne pas recourir à leurs services, n'est pas suffisant. Le fait qu'un acteur privé puisse définir de manière unilatérale les limites de la liberté d'expression de centaines de millions de personnes n'est pas une situation normale.

Si les plateformes soumettaient leur politique à l'avis de leurs utilisateurs, ainsi qu'à celui d'acteurs organisés tels que des associations de défense de la liberté d'expression ou des associations familiales, leur légitimité en serait confortée. Certaines plateformes présentent leur politique comme des « *community standards* », des règles de vie de la communauté des utilisateurs ; il s'agit de les prendre au mot et d'impliquer réellement cette communauté dans l'élaboration

des standards, aujourd'hui définis par les seules directions des entreprises. Cela devrait être d'autant plus aisé que l'univers d'internet est familier des processus d'élaboration participatifs, notamment en matière de standards techniques.

Imposer cette participation par la loi ne paraît pas adapté. La concertation doit être d'une ampleur proportionnée à l'importance de la plateforme : les attentes ne peuvent être identiques à l'égard d'un site qui vient d'être créé et d'une plateforme ayant plusieurs centaines de millions d'utilisateurs. Chaque plateforme doit être libre de définir les processus participatifs qui lui paraissent les plus adaptés. Dès lors, le droit souple est le plus approprié pour promouvoir la concertation sur les politiques des plateformes. Il pourrait s'agir, comme évoqué dans la proposition n° 6, d'une charte d'engagements signée par les plateformes et les parties prenantes.

Les pouvoirs publics n'auraient pas vocation à participer directement à l'élaboration de ces règles éditoriales. En revanche, ils pourraient énoncer des recommandations sur le contenu et le processus d'élaboration de ces règles et décerner un label à celles qui respectent les recommandations. Ce rôle pourrait être exercé par l'autorité de régulation compétente pour les contenus en cause.

Proposition n° 10 : Développer la participation des utilisateurs des plateformes à l'élaboration des règles définissant les contenus pouvant être mis en ligne sur leur site.

***Vecteur** : droit souple (charte d'engagements des plateformes) ; recommandations de l'autorité de régulation compétente.*

Développer la délibération collective sur les enjeux éthiques liés au numérique

Les évolutions technologiques liées au numérique soulèvent nombre de questions d'ordre éthique. Comme en matière de bioéthique, les possibilités d'actions nouvelles ouvertes par la technique amènent la société à s'interroger sur les valeurs dont elle souhaite imposer le respect et sur les possibles atteintes à la dignité de la personne humaine. Tout ce qui devient techniquement possible ne doit pas nécessairement être permis. Comme il a été vu ci-dessus, le développement du *Big Data* et des algorithmes prédictifs conduit à lever le « *voile d'ignorance* » qui entourait les caractéristiques de chaque individu et potentiellement à défaire nombre de solidarités implicites liées à cette ignorance, par exemple en matière d'assurance ou de sécurité sociale. Il serait légitime d'avoir un débat démocratique approfondi sur les perspectives et les enjeux éthiques de « *l'humanité augmentée* », c'est-à-dire d'une amélioration des performances physiques ou cognitives de l'être humain par la technique[487].

487. Cf. dans cette perspective l'avis n° 122 du Conseil consultatif national de l'éthique (CCNE) du 12 février 2014, intitulé *Recours aux techniques biomédicales en vue de « neuro-amélioration » chez la personne non malade: enjeux éthiques*, qui se penche notamment sur

De telles questions ne peuvent être abordées de manière satisfaisante dans des cercles étroits d'experts. Plusieurs scientifiques dont le physicien britannique Stephen Hawking se sont récemment inquiétés de la faiblesse de la réflexion collective sur les progrès de l'intelligence artificielle[488]. Depuis les années 1980, la bioéthique a su trouver ses modes de délibération permettant aux experts de dialoguer avec la société, au sein du Comité consultatif national d'éthique (CCNE) pour les sciences de la vie et de la santé, créé en 1983, et dans le cadre des états généraux de la bioéthique, qui doivent désormais être organisés avant tout projet de réforme sur les problèmes éthiques et les questions de société soulevés par les progrès de la connaissance dans les domaines de la biologie, de la médecine et de la santé[489]. Le numérique doit trouver ses propres processus, adaptés à la diversité des questions qu'il soulève et à son emprise sans doute plus importante que celle de la bioéthique sur la vie quotidienne des individus.

Une mission permanente d'animation de la délibération collective sur les enjeux éthiques liés au numérique devrait donc être créée. Deux organismes seraient susceptibles de l'exercer, la CNIL ou le Conseil national du numérique. Dans les deux cas, une formation spécialisée dénommée « *éthique et numérique* » devrait être créée auprès de ces organismes, qui ne serait pas composée exclusivement d'experts du numérique mais inclurait aussi des représentants des principaux courants de pensée, à l'exemple du CCNE. L'organisme investi pourrait définir librement les modalités d'organisation de cette délibération collective (organisation de débats publics en ligne ou hors ligne, jurys citoyens, conférences de consensus, constitution de commission spécialisées, etc.), tout en rendant compte de son action au Parlement et au Gouvernement.

Proposition n° 11 : Confier à la CNIL ou au Conseil national du numérique une mission permanente d'animation de la délibération collective sur les enjeux éthiques liés au numérique.

Vecteur *: loi pour la CNIL, décret pour le CNNum.*

---

les questions soulevées par les mouvements « *post-humanistes* » ou « *trans-humanistes* », sans prendre position à ce stade.

488. S. Hawking, S. Russel, M. Tegmark et F. Wilczek, "Stephen Hawking: 'Transcendence looks at the implications of artificial intelligence - but are we taking AI seriously enough?", *The Independent*, 1er mai 2014.

489. Article L. 1412-1-1 du code de la santé publique, issu de la loi du 7 juillet 2011 relative à la bioéthique.

3.3. Redéfinir les instruments de la protection des droits fondamentaux et repenser le rôle des autorités publiques

3.3.1. Tirer les conséquences du passage à l'ère de l'économie des données personnelles

Le cadre juridique de la protection des données personnelles a été forgé à une époque où la circulation des données et leur valeur économique restaient limitées. L'intervention publique doit aujourd'hui assurer d'une part la sécurisation juridique des usages des données, en ce qu'il est un facteur de développement de l'économie numérique, et d'autre part un encadrement plus étroit des traitements présentant les risques les plus importants.

L'approche générale préconisée par cette étude conduit à adhérer à nombre de dispositions figurant dans le projet de règlement européen. Celles-ci sont récapitulées dans l'encadré ci-dessous. Les propositions qui suivent portent sur des sujets ne figurant pas dans le projet de règlement en l'état.

Les principales dispositions du projet de règlement européen rejoignant l'approche générale préconisée par l'étude du Conseil d'État

- La normalisation des politiques d'utilisation des données personnelles (article 13 *bis*).

- Le droit à la portabilité des données personnelles (article 15).

- L'encadrement du profilage (article 20).

- La protection des données dès la conception ou « *privacy by design* » (article 23).

- L'obligation de conservation d'une documentation retraçant l'ensemble des traitements effectués (article 28).

- L'explicitation de l'obligation de sécurité incombant au responsable du traitement (article 30).

- L'obligation de notification à l'autorité de contrôle et de communication à la personne des violations de données à caractère personnel (articles 31 et 32).

- L'obligation d'étude d'impact et de consultation préalable de l'autorité de contrôle pour les traitements présentant des risques particuliers (articles 33 et 34).

- L'obligation de désignation d'un délégué à la protection des données (article 35)

Sécuriser juridiquement les usages présentant des risques limités pour les droits fondamentaux

L'article 6 de la directive n° 95/46/CE prévoit aujourd'hui qu'un « *traitement ultérieur à des fins statistiques, historiques ou scientifiques* » n'est pas réputé incompatible avec les finalités initiales du traitement de données, pour autant que les États membres prévoient des garanties appropriées, notamment en empêchant « *l'utilisation des données à l'appui de mesures ou de décisions prises à l'encontre d'une personne* ». Cette disposition, transposée en des termes identiques à l'article 6 de la loi du 6 janvier 1978, garantit une liberté de réutilisation statistique des données, sans qu'y fasse obstacle la finalité initiale du traitement. Elle est propice au développement du *Big Data*, dont on a dit toutes les potentialités qu'il recèle pour l'économie numérique et la mise en œuvre efficace des politiques publiques.

La proposition de règlement est à cet égard plus ambiguë. La disposition garantissant la compatibilité du traitement statistique avec les finalités initiales a disparu de l'article 5 portant sur les principes relatifs au traitement des données. Une nouvelle disposition prévoit qu'un traitement réalisé à des fins statistiques, historiques ou scientifiques, est licite. Mais cette notion de licéité, définie par l'article 6, signifie seulement qu'il n'est pas nécessaire de rechercher le consentement des personnes concernées ou un autre fondement tel que l'intérêt légitime du responsable du traitement ; comme l'a relevé le G29 dans un avis du 2 avril 2013[490], cette question est distincte de celle du respect du principe de détermination des finalités. En outre, l'article 83 introduit une nouvelle condition propre aux traitements réalisés à des fins statistiques, historiques ou scientifiques, qui ne peuvent être mis en œuvre que si « *ces finalités ne peuvent être atteintes d'une autre façon par le traitement de données qui ne permettent pas ou ne permettent plus d'identifier la personne concernée* » ; la vérification de cette condition pourrait être complexe.

Les traitements statistiques ne présentent pas de risques pour les individus, sous réserve de veiller aux risques de réidentification (cf. *infra* 3.4.1), et leur libre développement revêt des enjeux économiques importants dans le contexte du *Big Data*. Il est donc souhaitable de revenir à des dispositions garantissant sans ambiguïté la liberté de réutilisation statistique des données, notamment en réintroduisant la présomption de compatibilité aujourd'hui prévue par l'article 6 de la directive et en supprimant la nouvelle condition prévue par l'article 83 du projet de règlement.

Proposition n° 12 : Afin de sécuriser le développement du *Big Data* en Europe, maintenir sans ambiguïté dans la proposition de règlement européen la liberté de réutilisation statistique des données personnelles, quelle que soit la finalité initiale de leur traitement, en prévoyant pour seule condition que cette réutilisation soit entourée de garanties d'anonymat appropriées.

Vecteur *: le règlement de l'Union européenne.*

490. Article 29, *Data Protection Working Party*, *Opinion 03/2013 on purpose limitation*, 2 avril 2013, 00569/13/EN WP 203.

L'article 11 de la loi du 6 janvier 1978 dispose que la CNIL « *informe toutes les personnes concernées et tous les responsables de traitements de leurs droits et obligations* » et « *conseille les personnes et organismes qui mettent en œuvre ou envisagent de mettre en œuvre des traitements automatisés de données à caractère personnel* ». La CNIL développe depuis plusieurs années, comme le met en exergue son rapport d'activité pour 2012, une action d'accompagnement des responsables de traitement dans leurs démarches de conformité à la réglementation. Pourtant, la CNIL reste d'avantage perçue comme une autorité de contrôle, dont la raison même serait de restreindre l'utilisation des données personnelles. Sans remettre en cause sa mission essentielle de contrôle et de sanction, son rôle de conseil et d'accompagnement pourrait encore d'avantage être mis en avant. La récente création d'une direction de la conformité, avec en son sein des secteurs organisés par type de responsable de traitement (organismes publics, entreprises), va dans ce sens. Les usagers de la CNIL sont les personnes dont les données doivent être protégées, mais ce sont aussi les responsables de traitement qui cherchent de bonne foi à respecter la législation.

Durant la phase séparant l'adoption définitive du règlement européen de son entrée en vigueur, qui devrait durer deux ans, une attention particulière devrait être portée à l'accompagnement des responsables de traitement, qui devront veiller à se conformer aux nombreuses nouveautés que comporte ce texte.

Proposition n° 13 : Renforcer le rôle de conseil et d'accompagnement des responsables de traitement par la CNIL.

Vecteur *: action de la CNIL*

La création d'un rescrit en matière de données personnelles serait un instrument adapté pour renforcer la sécurité juridique des porteurs de projets. En effet, peu de traitements sont soumis à autorisation préalable et le responsable de traitement doit donc apprécier lui-même la licéité de son action, avec le risque de se voir infliger une sanction s'il a mal compris ses obligations. Certaines notions, comme l'intérêt légitime du responsable de traitement qui doit être mis en balance avec les droits fondamentaux de la personne concernée en vertu de l'article 7 de la loi du 6 janvier 1978, peuvent être d'interprétation délicate. Dans le cadre du rescrit, le responsable de traitement solliciterait une prise de position de la CNIL sur la licéité de son traitement ; la réponse donnée par la CNIL lui serait opposable, à condition que le responsable de traitement ait communiqué toutes les informations nécessaires. Dans son étude *Le rescrit : sécuriser les initiatives et les projets*[491], le Conseil d'État a estimé que le rescrit pourrait notamment être développé pour prévenir des sanctions administratives : le « *rescrit données personnelles* » s'inscrirait dans cette hypothèse. Il mettrait également en œuvre

491. Les études du Conseil d'État, La documentation Française, mars 2014.

la proposition du Conseil de simplification de la vie des entreprises[492], tendant de manière générale à développer le rescrit – dénommé « *réponse garantie* » – dans les relations entre l'administration et les entreprises. Ce mécanisme s'apparentant à un *certificat de conformité*, il pourrait recevoir cette qualification, mieux connue en droit européen que celle du rescrit.

Proposition n° 14 : Créer un *certificat de conformité (rescrit « données personnelles »*).

Vecteur *: loi.*

Le projet de règlement européen définit des catégories de traitement présentant des risques particuliers, soumis à deux obligations spécifiques : la réalisation d'une étude d'impact et la consultation préalable de l'autorité de contrôle[493]. Le champ de ce régime d'encadrement renforcé est cependant entaché d'importantes incertitudes, dans le texte de la Commission comme dans celui du Parlement européen. L'existence d'une obligation de consultation préalable dépend du résultat de l'étude d'impact : l'autorité de contrôle devra être saisie si « *une analyse d'impact (…) indique que les traitements sont, du fait de leur nature, de leur portée ou de leurs finalités, susceptibles de présenter un degré élevé de risques particuliers* » ; il n'existe pas de définition objective du « *degré élevé de risques particuliers* » et il reviendrait au responsable de traitement d'apprécier si son étude d'impact justifie la saisine de l'autorité, au risque de s'exposer à des lourdes sanctions si son appréciation est erronée. En outre, le texte du Parlement européen définit une architecture complexe à deux niveaux, dans laquelle le responsable de traitement doit réaliser une « *analyse du risque* », qui peut donner lieu selon ses résultats à une analyse d'impact.

Il est très souhaitable de définir d'emblée dans le règlement les catégories de traitement soumises aux obligations d'étude d'impact et de consultation préalable de l'autorité de contrôle. La liste des catégories de traitement à risques particuliers qui figure dans le projet de règlement apparaît globalement pertinente, même si certains items peuvent être discutés (en particulier, le seuil de 5 000 personnes concernées par le traitement apparaît assez bas)[494]. Chaque responsable de

492. Créé par le décret n° 2014-11 du 8 janvier 2014, pour une durée de trois ans, le Conseil de la simplification pour les entreprises est chargé de proposer au Gouvernement les orientations stratégiques de la politique de simplification à l'égard des entreprises.

493. Cette « *consultation préalable* » est une formalité d'autant plus importante que l'autorité de contrôle peut s'opposer au traitement : selon l'article 34.3, « *lorsque l'autorité de contrôle compétente détermine, conformément à ses attributions, que le traitement prévu n'est pas conforme au présent règlement, en particulier lorsque les risques ne sont pas suffisamment identifiés ou atténués, elle interdit le traitement prévu et formule des propositions appropriées afin de remédier à cette non-conformité* ».

494. Dans le texte voté par le Parlement européen, la liste prévue par l'article 32 *bis* est la suivante : le traitement de données à caractère personnel de plus de 5 000 personnes concernées sur une période de douze mois consécutifs ; le traitement des catégories particulières de

traitement pourra ainsi savoir, en fonction de la nature de son activité, quelle est la teneur de ses obligations. La liste fixée par le règlement pourrait être complétée par un acte délégué de la Commission.

Proposition n° 15 : Clarifier le champ des traitements soumis en raison de leurs risques à des obligations particulières telles que la réalisation d'une étude d'impact ou la consultation préalable de l'autorité de contrôle, en définissant dans le règlement la liste des catégories de traitement concernées. La soumission à l'obligation de consultation préalable ne doit pas dépendre du résultat de l'étude d'impact.

Vecteur *: règlement de l'Union européenne.*

Les textes actuels (article 27 de la directive n° 95/46/CE et 3° de l'article 11 de la loi du 6 janvier 1978) prévoient déjà l'existence de codes de conduite professionnels pouvant être soumis à l'examen des autorités de contrôle nationales ou du G29. Le projet de règlement comporte des dispositions similaires. À ce jour, les codes de conduite sont cependant restés assez peu développés.

Le développement de la corégulation présenterait pourtant plusieurs intérêts. Il permettrait de décliner les implications techniques et sectorielles des principes définis par le règlement, en évitant à celui-ci d'entrer dans des précisions excessives. Il favoriserait l'appropriation des exigences de protection des données personnelles par les acteurs professionnels.

Afin de stimuler l'adoption de codes de conduite, le règlement pourrait prévoir une procédure d'homologation. L'homologation, délivrée par l'autorité de contrôle nationale pour les codes nationaux et par le Comité européen à la protection des données (CEPD), successeur du G29, pour les codes européens, serait soumise aux conditions suivantes : le code de conduite doit préciser les modalités de mise en œuvre de la législation ou proposer un niveau de protection supérieur ; il doit avoir été élaboré de manière transparente en impliquant les parties prenantes ; il doit prévoir les modalités d'évaluation de sa mise en œuvre par les acteurs professionnels concernés, cette évaluation ne se substituant pas aux contrôles

---

données à caractère personnel visées à l'article 9, paragraphe 1 (« *données sensibles* »), des données de localisation, ou des données relatives à des enfants ou des employés dans des fichiers informatisés de grande ampleur ; l'établissement de profils sur la base desquels sont prises des mesures produisant des effets juridiques concernant ou affectant de manière tout aussi significative ladite personne ; le traitement de données à caractère personnel destinées à la fourniture de soins de santé, à des recherches épidémiologiques ou à des études relatives à des maladies mentales ou infectieuses, lorsque les données sont traitées aux fins de l'adoption de mesures ou de décisions à grande échelle visant des personnes précises ; la surveillance automatisée à grande échelle de zones accessibles au public ; lorsqu'une violation des données à caractère personnel risque de porter atteinte à la protection des données à caractère personnel, de la vie privée, des droits ou des intérêts légitimes de la personne concernée.

exercés par les autorités de contrôle. En contrepartie, le respect d'un code de conduite homologué serait un des critères retenus par l'autorité de contrôle pour ses décisions d'autorisation ou de sanction.

Proposition n° 16 : Créer une procédure d'homologation des codes de conduite professionnels élaborés au niveau national ou européen.

Vecteur *: règlement de l'Union européenne.*

Les textes actuels (article 17 de la directive n° 95/46/CE et article 34 de la loi du 6 janvier 1978) définissent une obligation générale de sécurité des traitements de données, mais ne précisent pas ses implications. La responsabilité de définir les mesures de sécurité adéquates est ainsi entièrement laissée aux responsables de traitement. Face aux risques croissants liés à la cybercriminalité, cette approche n'apparaît plus suffisante.

Le projet de règlement voté par le Parlement européen précise quelque peu les obligations qui incombent aux responsables de traitement mais ne comble pas le vide quant aux implications techniques de ces obligations, ce qui n'est d'ailleurs pas son rôle. Il y a ici place pour une approche bien connue du législateur européen, consistant à définir dans un texte de base (règlement ou directive) les obligations générales et à renvoyer à des normes techniques les spécifications précises. Les responsables de traitement se soumettant à ces normes seraient présumés s'acquitter de leur obligation générale de sécurité. Les normes relatives à la sécurité des traitements de données personnelles pourraient être en grande partie communes avec les normes relatives à la sécurité des systèmes d'information, que la proposition de directive du 7 février 2013 concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et de l'information dans l'Union, souvent dénommée « *directive cybersécurité* », prévoit de développer.

Proposition n° 17 : Développer la normalisation en matière de sécurité des traitements de données personnelles.

Vecteur *: règlement de l'Union européenne.*

Le projet de règlement prévoit une période de deux ans entre sa publication et son entrée en vigueur. Si le règlement est définitivement adopté, cette période de transition devra être pleinement mise à profit pour que les acteurs se préparent à appliquer les nouvelles dispositions. L'ensemble des responsables de traitement devront en effet s'assurer de la conformité de leurs opérations au nouveau cadre juridique. Nombre d'entre eux seront conduits à se doter d'un délégué à la protection des données (DPD), soit à partir du rôle aujourd'hui joué par le « correspondant informatique et libertés » (CIL), soit *ex nihilo*, à réaliser des études d'impact ou à notifier les traitements considérés comme les plus risqués à l'autorité de contrôle.

Les pouvoirs publics auront un rôle à jouer pour anticiper et accompagner cette transition. En particulier, un important besoin en délégués à la protection des données est à prévoir[495], qui pourrait nécessiter la mise en place de programmes spécifiques de formation. Une organisation de la transition, reposant sur une coopération entre le gouvernement, la CNIL et les principaux acteurs professionnels concernés, devrait être définie.

Proposition n° 18 : Anticiper et organiser la transition vers le nouveau cadre juridique issu du règlement, par une coopération entre le gouvernement, la CNIL et les principaux acteurs professionnels concernés.

Vecteur *: action du gouvernement, de la CNIL et des principaux acteurs professionnels concernés.*

Proportionner l'encadrement au degré de risque du traitement

Les textes actuels ne prévoient de procédure de certification de la conformité d'un traitement de données à la législation qu'à titre volontaire, dans le cadre de la délivrance d'un label par la CNIL (3° de l'article 11 de la loi du 6 janvier 1978). Le projet de règlement européen maintient cette approche.

Il serait pourtant pertinent de rendre la certification obligatoire pour les catégories de traitement présentant les risques les plus importants. La certification permet en effet de vérifier de manière continue le respect de la législation, ce qui complète l'examen *a priori* par l'autorité de contrôle dans le cadre de la procédure de consultation préalable. La certification de la conformité serait effectuée de manière périodique par un organisme tiers indépendant, accrédité par l'autorité de contrôle ; elle serait effectuée aux frais du responsable de traitement. L'obligation de certification pourrait concerner certaines catégories de traitements présentant des risques particulièrement importants, par exemple les traitements de données sensibles ou ceux impliquant la surveillance automatisée de zones accessibles au public.

Proposition n° 19 : Créer pour les catégories de traitements présentant les risques les plus importants une obligation de certification périodique (complétant l'examen *a priori* par l'autorité de contrôle dans le cadre de la procédure de consultation préalable) par un organisme tiers indépendant et accrédité par l'autorité de contrôle.

Vecteur *: règlement de l'Union européenne.*

495. Le secteur public est d'ailleurs particulièrement concerné, car le projet de règlement y rend obligatoire la présence d'un DPD, alors qu'en France, peu d'organismes publics sont aujourd'hui dotés d'un CIL.

La transmission de données personnelles d'une entité à une autre, notamment lorsqu'elle se fait à titre onéreux, nécessite une attention particulière : dès lors que les données sont transmises à un acteur autre que celui qui les a initialement collectées, il existe un risque d'utilisation incompatible avec les finalités de cette collecte. Le risque s'accroît à chaque nouvelle cession, situation fréquente à l'ère du marché des données personnelles. Cette attention particulière devrait se traduire par trois mesures : l'inscription dans la loi du principe, dégagé par la jurisprudence, de nullité des transactions portant sur des fichiers non déclarés à la CNIL (a) ; l'incitation à tenir une comptabilité de ces transactions (b) ; la recommandation de fournir aux personnes exerçant leur droit d'accès une liste complète des entités auxquelles leurs données ont été communiquées (c). Ces deux dernières mesures figureraient dans un code de conduite professionnel homologué (v. proposition n° 16).

(a) En jugeant dans un arrêt du 25 juin 2013 que les transactions portant sur des fichiers non déclarés à la CNIL étaient nulles[496], la Cour de cassation a posé les jalons d'un encadrement particulier des cessions de données personnelles. Cette jurisprudence pourrait être codifiée par le législateur afin de lui donner une plus grande sécurité juridique fondée sur le principe conventionnel de prévisibilité de la loi. La loi devrait préciser que l'obligation de déclaration de la transaction elle-même[497] est également sanctionnée de nullité. Compte tenu de ses lourdes conséquences pour les parties à la transaction, la nullité devrait inciter à un meilleur respect de l'obligation de déclaration à la CNIL, donnant à celle-ci une vue plus complète des échanges de données et l'aidant ainsi à cibler ses contrôles. Les mêmes conséquences devraient s'appliquer *a fortiori* aux traitements soumis à autorisation et qui ne l'ont pas été.

Si le règlement européen est définitivement adopté, l'obligation de déclaration disparaîtra. La nullité ne concernerait alors plus que les transactions portant sur des fichiers soumis à une obligation de consultation préalable de l'autorité de contrôle.

(b) Les entités procédant de manière récurrente à des transactions portant sur des données personnelles pourraient être invitées à tenir un registre de ces transactions. Cette incitation serait une déclinaison particulière de l'obligation générale de documentation prévue par le projet de règlement européen, qui implique de retracer l'ensemble des traitements de données mis en œuvre. Elle faciliterait l'exercice de la mission des autorités de contrôle.

(c) L'article 39 de la loi du 6 janvier 1978 impose de communiquer à la personne exerçant son droit d'accès des informations relatives « *aux destinataires ou aux catégories de destinataires auxquels les données sont communiquées* ». Cette

496. Com. 25 juin 2013, n° 12-17.037.

497. En effet, la transaction constitue elle-même un traitement de données, puisque l'article 2 de la loi du 6 janvier 1978 range parmi les traitements « *la communication par transmission, diffusion ou toute autre forme de mise à disposition* ». Dès lors que le transfert de fichiers est effectué par voie électronique, elle constitue un traitement automatisé de données, la CJUE ayant une conception très large de la notion de traitement automatisé (cf. CJCE 6/11/2003, *Bodil Lindqvist*, C-101/01, § 26). Tous les traitements automatisés de données personnelles devant être déclarés à la CNIL, les transactions portant sur des données personnelles doivent être déclarées.

formulation n'impose pas de donner la liste complète des entités auxquelles les données ont été cédées. Or cette information peut être d'un grand intérêt pour la personne exerçant son droit d'accès, car elle lui donne une idée plus précise de l'ampleur de la dissémination de ses données et lui permet de solliciter ces entités. Le droit d'accès pourrait utilement s'accompagner de la communication d'une liste complète des entités auxquelles les données ont été cédées.

Proposition n° 20 : Porter une attention particulière aux transmissions de données personnelles d'une entité à une autre en :

- codifiant dans la loi la jurisprudence relative à la nullité des transactions portant sur des fichiers non déclarés ou non autorisés à la CNIL (*vecteur : loi*) ;

- incitant les acteurs procédant de manière récurrente à de telles transactions à en tenir un registre (*vecteur : code de conduite professionnel*) ;

- incitant à fournir aux personnes exerçant leur droit d'accès une liste complète des entités auxquelles leurs données ont été communiquées (*vecteur : code de conduite professionnel*).

Réexaminer le régime juridique des numéros d'identification

La proportionnalité de l'encadrement au degré de risque du traitement implique de le renforcer pour les traitements présentant des risques particuliers. Il invite aussi à alléger des restrictions pouvant aujourd'hui paraître excessives. L'encadrement particulier de l'utilisation du numéro d'inscription au répertoire (NIR)[498], se justifiait au moment de l'adoption de la loi du 6 janvier 1978. En effet, le recours au NIR constituait alors le principal moyen d'interconnexion des fichiers, comme l'avait montré le projet « SAFARI » à l'origine de la loi. La situation est aujourd'hui différente. Même si le NIR reste un moyen de faciliter l'interconnexion en raison de sa fiabilité, il n'y est plus nécessaire. D'autre part, il faut souligner que des États dont le respect des droits fondamentaux ne peut être mis en doute n'appliquent pas du tout les mêmes restrictions à l'emploi de numéros nationaux d'identification [499].

498. « *Toute personne née en France métropolitaine et dans les départements d'outre-mer (DOM) est inscrite au répertoire national d'identification des personnes physiques (RNIPP). L'inscription à ce répertoire entraîne l'attribution du numéro d'inscription au répertoire (NIR) qui est utilisé notamment par les organismes d'assurance maladie pour la délivrance des « cartes vitales ». Ce numéro d'identification unique de l'individu est formé de 13 chiffres : le sexe (1 chiffre), l'année de naissance (2 chiffres), le mois de naissance (2 chiffres) et le lieu de naissance (5 chiffres). Les 3 chiffres suivants correspondent à un numéro d'ordre qui permet de distinguer les personnes nées au même lieu à la même période ; une clé de contrôle à 2 chiffres complète le NIR. Le NIR est communément appelé « numéro de sécurité sociale »* » (*source* : INSEE, www.insee.fr, *Définitions et méthodes*).

499. En Suède, le « *personnumer* », instauré en 1947, est un numéro d'identification signifiant inscrit dans les registres d'état civil. Il est indispensable pour toutes les démarches administratives et est largement utilisé dans les démarches privées. Au Danemark, le « *Det Centrale Person Register* » a été créé en 1968 et ses utilisations sont tout aussi larges.

Les différences entre les législations des États européens en matière de numéros d'identification expliquent que la directive 95/46/CE leur ait laissé toute latitude sur ce point (article 8.7 : « *Les États membres déterminent les conditions dans lesquelles un numéro national d'identification ou tout autre identifiant de portée générale peut faire l'objet d'un traitement.* »).

Cependant, en France, l'utilisation du NIR suscite historiquement de fortes appréhensions pour la protection de la vie privée principalement en raison de son caractère signifiant : il fournit en effet des informations sur le sexe, l'année et le mois de naissance ainsi que le lieu de naissance.

Si un identifiant national non signifiant, généré de manière aléatoire pour chaque personne, était instauré en complément ou en substitut au NIR, il serait envisageable d'encadrer son utilisation de manière moins stricte. Il convient donc de mettre à l'étude la création d'un numéro unique d'identification en évaluant son intérêt pour la conduite des politiques publiques et la simplification des démarches administratives des citoyens, au regard de son coût et des risques qui demeureraient pour la vie privée en dépit du caractère non signifiant.

Proposition n° 21 : Mettre à l'étude la création d'un numéro national unique d'identification non signifiant.

Vecteur *: action du Gouvernement et de la CNIL.*

L'encadrement du NIR prévu par la loi est un obstacle à certains traitements d'utilité publique ne présentant pas de risques pour la vie privée. En matière de santé, des chercheurs souhaitent rapprocher les données collectées dans le cadre d'enquêtes de celles figurant dans des bases de données administratives telles que le SNIIRAM[500]. Cette opération devant être autorisée par un décret en Conseil d'État pris après avis de la CNIL, la lourdeur de la procédure est susceptible de décourager les projets de recherche[501] et apparaît d'autant moins justifiée que les traitements de données personnelles ayant pour fin la recherche dans le domaine de la santé doivent être autorisés par la CNIL en vertu du chapitre IX de la loi du 6 janvier 1978. En l'absence de numéro national unique d'identification non signifiant, l'utilisation du NIR devrait donc être permise pour les traitements ayant pour fin la recherche dans le domaine de la santé, lorsqu'ils ont été autorisés par la CNIL dans le cadre du chapitre IX. Pour ces traitements, la loi devrait prévoir une dérogation aux dispositions de l'article 27 de la loi qui exigent un décret en Conseil d'État ou un arrêté pris après avis de la CNIL en plus de l'autorisation accordée par cette dernière.

En dehors de l'Europe, la Corée du sud utilise un numéro de résident à 13 chiffres. En 2006, elle a créé un autre numéro moins signifiant, dit « *I-PIN* », dans le but d'inciter les personnes à l'utiliser dans leurs démarches personnelles.

500. Système national d'information inter-régimes de l'assurance-maladie : cf. l'annexe n° 3.

501. Cf. sur ce point P.-L. Bras et A. Loth, *Rapport sur la gouvernance et l'utilisation des données de santé*, septembre 2013.

Cette modification législative complèterait le changement de doctrine d'utilisation du NIR annoncé par la CNIL dans son rapport d'activité pour 2013 : la CNIL admet désormais que le NIR soit utilisé comme identifiant national pour les données de santé, alors qu'elle avait jusqu'ici toujours affirmé la nécessité d'un « *cantonnement* » au domaine de la sécurité sociale.

Proposition n° 22 : Permettre le recours au NIR pour les traitements de données personnelles ayant pour fin la recherche dans le domaine de la santé et autorisés par la CNIL en vertu du chapitre IX de la loi du 6 janvier 1978. Admettre l'utilisation du NIR comme identifiant national pour les données de santé, aux fins de faciliter les politiques publiques de recherche et de prévention.

Vecteur *: loi ; action de la CNIL.*

3.3.2. Définir un droit des algorithmes prédictifs

L'étude propose ici des principes généraux ayant vocation à régir la conception et la mise en œuvre des algorithmes, puis des recommandations concernant deux domaines d'utilisation particuliers, dans le commerce en ligne et dans les industries culturelles.

Définir des principes d'intervention humaine effective, de transparence et de non-discrimination

L'article 10 de la loi du 6 janvier 1978 interdit qu'une décision produisant des effets juridiques à l'égard d'une personne soit prise « *sur le seul fondement d'un traitement automatisé de données destiné à définir le profil de l'intéressé ou à évaluer certains aspects de sa personnalité* ». Le développement des algorithmes donne aujourd'hui toute sa pertinence à cette disposition, qui existait déjà dans le texte initial de la loi. Pour que cette interdiction ne soit pas que formelle, il faut cependant éviter que des systèmes présentés comme relevant de « *l'aide à la décision* » soient en réalité presque toujours suivis et commandent la décision, l'intervention humaine n'étant alors qu'apparente.

Une recommandation de la CNIL ou un avis du G29 pourrait préciser l'interprétation du texte actuel, en prévoyant que l'intervention humaine ne doit pas être que formelle. Cette disposition pourrait indiquer les critères permettant de s'assurer du caractère effectif de cette intervention, tels que les compétences et les qualifications de la personne qui prend la décision, la marge de manœuvre dont elle dispose dans les processus définis par son organisation et l'existence d'éléments d'information lui permettant le cas échéant de justifier la prise d'une autre décision que celle proposée par l'algorithme. La recommandation ou l'avis pourrait aussi préconiser la tenue par l'organisme concerné de statistiques sur le taux de suivi de la proposition de l'algorithme, qui constitue un bon indicateur du caractère effectif de l'intervention humaine.

Proposition n° 23 : Pour assurer l'effectivité de l'interdiction de fonder une décision sur la seule mise en œuvre d'un traitement automatisé, confirmer que l'intervention humaine dans la décision doit être réelle et pas seulement formelle. Indiquer dans un instrument de droit souple les critères d'appréciation du caractère effectif de l'intervention humaine.

Vecteur *: règlement de l'Union européenne et droit souple (recommandation de la CNIL ou avis du G29).*

Lorsqu'une décision produisant des effets juridiques ou une mesure affectant de manière significative les intérêts d'une personne est en partie fondée sur un algorithme, cette personne devrait bénéficier de garanties analogues à celles d'une procédure contradictoire. Elle doit en effet être en mesure de faire valoir ses observations auprès de la personne qui prendra la décision, en produisant des arguments de nature le cas échéant à contrebalancer la proposition de l'algorithme.

À cette fin, l'auteur de la décision devrait d'abord informer la personne faisant l'objet de celle-ci des données personnelles utilisées par l'algorithme, ce qui lui permettra de s'assurer de leur véracité ; le meilleur des algorithmes ne peut en effet produire que des résultats erronés si les données qui lui sont soumises sont inexactes… Il devrait aussi lui présenter la logique générale de l'algorithme, en expliquant par exemple, pour un organisme de crédit, que telle information est utilisée en raison de la corrélation observée par des études avec le risque de défaut. Enfin, comme indiqué, la personne devrait avoir la possibilité de faire valoir ses observations avant la prise de décision[502].

Proposition n° 24 : Imposer aux auteurs de décisions s'appuyant sur la mise en œuvre d'algorithmes une obligation de transparence sur les données personnelles utilisées par l'algorithme et le raisonnement général suivi par celui-ci. Donner à la personne faisant l'objet de la décision la possibilité de faire valoir ses observations.

Vecteur *: loi ou règlement de l'Union européenne.*

Il est souvent avancé que les algorithmes sont des « *boîtes noires* » impossibles à contrôler, tant en raison du secret industriel qui les protège que de leur complexité technique. Cette affirmation n'est pas exacte. En effet, il est toujours possible de tester les résultats de l'algorithme : sans qu'il soit besoin de connaître le fonctionnement interne de l'algorithme, la soumission d'une multitude de

502. Dans le texte actuel du règlement, le fait que la personne ait pu faire valoir ses observations est une des conditions pour que le traitement ne soit pas considéré comme fondé uniquement sur un traitement automatisé de données. La proposition tend à garantir le droit de faire valoir ses observations dès lors qu'il existe un algorithme d'aide à la décision, même lorsqu'il est établi que la décision n'est pas fondée exclusivement sur cet algorithme.

données entrantes et l'observation statistique des résultats permet de déceler ses caractéristiques. Ainsi, il est possible de déterminer si un moteur de recherche favorise les services qui lui sont affiliés en lui soumettant de multiples requêtes et en observant les résultats proposés, sans qu'il soit nécessaire de connaître son algorithme. Cette approche dite « *d'ingénierie inversée* » a par exemple permis d'établir des discriminations illicites dans les algorithmes de moteurs de recherche : une chercheure de l'université de Harvard[503] a montré que la saisie de noms fréquemment portés dans la population noire renvoyait beaucoup plus souvent à des publicités suggérant qu'elles avaient été détenues[504] que la saisie de noms fréquemment portés dans la population blanche.

Deux conséquences doivent en être déduites. D'une part, la CNIL doit disposer de moyens adéquats pour contrôler les algorithmes. Sur le plan juridique, l'article 44 de la loi du 6 janvier 1978, qui permet aux membres de la Commission et aux agents de contrôle « *d'accéder aux programmes informatiques et aux données* », lui donne déjà les prérogatives nécessaires. Sur le plan humain, il apparaît nécessaire de continuer à renforcer les moyens de la CNIL par le recrutement de spécialistes dotés de compétences adéquates. Les formations de « *data scientists* » créées au cours des dernières années par de nombreuses grandes écoles peuvent y pourvoir. Des rémunérations attractives devront certes être proposées pour faire venir dans un organisme public des profils très demandés par nombre d'entreprises privées. Cet effort devrait cependant être consenti, car la puissance publique ne peut exercer un contrôle efficace si l'asymétrie des compétences joue de manière trop importante en sa défaveur.

D'autre part, la méthode d'ingénierie inversée devrait aider à appréhender les discriminations fondées sur l'utilisation des données personnelles. L'interdiction de la collecte et du traitement des données sensibles (origines raciales ou ethniques, opinions politiques, philosophiques ou religieuses, appartenance syndicale, santé ou vie sexuelle) a été conçue comme une garantie contre la discrimination. Cependant, il est aujourd'hui possible de reconstituer ces informations à partir de données en apparence anodines (sites consultés, lieux fréquentés, termes saisis dans des moteurs de recherche). L'ingénierie inversée permet de repérer les usages discriminatoires de ces données indirectement personnelles.

Proposition n° 25 : Dans le cadre de l'article 44 de la loi du 6 janvier 1978 et dans le respect du secret industriel, développer le contrôle des algorithmes par l'observation de leurs résultats, notamment pour détecter des discriminations illicites, en renforçant à cette fin les moyens humains dont dispose la CNIL.

Vecteur *: action de la CNIL.*

503. L. Sweeney, « Discrimination in Online Ad Delivery », janvier 2013, http://dataprivacylab.org/projects/onlineads/1071-1.pdf.

504. Aux États-Unis, des sociétés commercialisent des informations sur l'historique judiciaire de tout un chacun ; ceci explique qu'un moteur de recherche puisse proposer des publicités suggérant que la personne a été détenue lorsqu'une requête sur le nom d'une personne lui est présentée.

Réguler la mise en œuvre des algorithmes en matière de commerce en ligne et d'industries culturelles

Ainsi qu'il l'a été dit précédemment (cf. 2.2.4), la dissémination des données personnelles et le développement du commerce en ligne favorise la différenciation des prix. Des signaux tels que l'obtention d'un brevet par *Google* pour une technique de différenciation des prix ou les débats concernant la pratique de « *l'IP tracking* » suggèrent que de telles différenciations pourraient effectivement se développer. Toutefois, l'adoption d'une législation prohibant des pratiques de différenciation par les prix n'est pas recommandée à ce stade. D'une part, l'information sur leur développement effectif n'est pas suffisante. D'autre part, la différenciation des prix n'est pas illicite par nature (par exemple, les pratiques de fidélisation de la clientèle, les offres commerciales ou les tarifs réduits proposés à certaines catégories de la population comme les jeunes). La réflexion sur les critères de la distinction entre pratiques licites et illicites doit donc être approfondie. La transparence du système de différentiation mis en place pourrait notamment y contribuer. L'article L. 113-3 du code de la consommation imposant l'information du consommateur sur les prix pourrait fonder une telle exigence de transparence.

Dans le même but, un programme d'enquêtes de la DGCCRF pourrait être défini et le Conseil national de la consommation, où sont représentés les professionnels, les consommateurs et les pouvoirs publics, pourrait se voir confier une mission de réflexion sur le sujet.

À l'issue de cette phase d'études, un texte législatif pourrait préciser quelles formes de différenciation des prix constituent des pratiques commerciales illicites ou déloyales et les sanctions administratives ou pénales dont elles feraient l'objet.

Proposition n° 26 : Analyser les pratiques de différenciation des prix reposant sur l'utilisation des données personnelles, mesurer leur développement et déterminer celles qui devraient être qualifiées de pratiques commerciales illicites ou déloyales, et sanctionnées comme telles.

Vecteur *: action de la DGCCRF ; saisine du Conseil national de la consommation et de l'Autorité de la concurrence ; loi à l'issue de la réflexion.*

La promotion de la diversité culturelle conserve toute sa pertinence à l'ère du numérique. Elle justifie que l'exercice de la liberté de communication ou de la liberté d'entreprendre dans certains secteurs d'activité soit subordonné au respect d'obligations destinées à soutenir cette diversité.

Les obligations de soutien financier à la production ne sont pas affectées dans leur principe par le numérique : rien n'interdit, comme l'a fait le décret du 12 novembre 2010 relatif aux services de médias audiovisuels à la demande (SMAD), d'imposer aux fournisseurs de contenus culturels sur internet de participer à ce financement, selon des modalités similaires à celles existant pour les autres canaux de diffusion (télévision, radio, cinéma). La principale difficulté tient à la possibilité pour ces fournisseurs de diffuser leurs contenus en France tout en étant établis depuis d'autres pays à la

réglementation moins exigeante ; un risque de concurrence par le moins-disant existe. Afin de le combattre, une harmonisation renforcée au sein de l'Union européenne ou le passage du principe du pays d'origine à celui du pays de destination, comme le préconise la France, apparaissent souhaitables (cf. *supra* 2.3.1).

L'obligation de réserver une proportion du catalogue à des œuvres françaises ou européennes, qui constitue l'autre pilier du soutien à la diversité culturelle, apparaît en revanche inadaptée dans son principe aux modes de diffusion sur internet. Si elle conserve tout son sens pour les programmes linéaires diffusés par les chaînes de radio et de télévision, elle ne peut exercer qu'une influence limitée sur les contenus effectivement choisis par l'internaute sur des sites de vidéo ou de musique en ligne. Conçue dans un univers de rareté, la logique des quotas est peu pertinente dans celui de la surabondance des contenus culturels que nous connaissons aujourd'hui.

La réglementation actuelle ne saisit pas le rôle pourtant essentiel joué par les algorithmes de recommandation, qui sont au cœur du succès des sites de vidéo à la demande, de musique en ligne et des plateformes de partage de contenus. Par construction, les algorithmes de recommandation utilisés par les plateformes tendent à se fonder sur l'observation des préférences passées et sur les corrélations entre les préférences des utilisateurs. Ces mécanismes présentent une grande efficacité pour assurer la satisfaction immédiate de l'utilisateur, mais elles ne favorisent pas la découverte de contenus culturels dont celui-ci n'est pas familier.

Une première piste consisterait à imposer aux acteurs concernés d'agir sur leurs algorithmes, en favorisant la prise en compte des critères de promotion de la diversité culturelle. Les plateformes auraient le choix des moyens de cette prise en compte : elle pourrait passer par la bonification dans l'algorithme des œuvres françaises ou européennes, ou par la mise en place d'une fenêtre dédiée à ces œuvres dans le résultat des recommandations. Toutefois, une telle obligation devrait être prévue par le droit de l'Union européenne, le cadre actuel ne le permettant pas, ni pour les SMAD[505] ni pour les plateformes[506]. Elle présenterait en outre un caractère intrusif dans l'exercice de la liberté de recommandation de ces sites.

Il apparaît donc préférable de recourir au droit souple ou à la contractualisation, en travaillant avec les sites concernés sur des engagements volontaires en matière de soutien à la diversité culturelle. Ces engagements, qui pourraient notamment être inscrits dans les conventions dont le CSA préconise la création (cf. *supra* 2.2.3), devraient traiter de la prise en compte de la diversité culturelle dans les algorithmes de recommandation.

---

505. Selon l'article 13.1 de la directive SMA, « *les États membres veillent à ce que les services de médias audiovisuels à la demande fournis par des fournisseurs de services de médias relevant de leur compétence promeuvent, lorsque cela est réalisable et par des moyens appropriés, la production d'œuvres européennes ainsi que l'accès à ces dernières* ». Si cette disposition ne définit pas de manière limitative les mesures pouvant être prises par les États, l'expression « *veillent à* » paraît un peu faible pour autoriser une mesure restreignant la liberté de recommandation des sites concernés.

506. Une telle obligation constituerait en effet une « *exigence relative à l'exercice de l'activité d'un service de la société de l'information* », qui devrait dès lors être prévue par la directive sur le commerce électronique.

Proposition n° 27 : Encourager la prise en compte de la diversité culturelle dans les algorithmes de recommandation utilisés par les sites internet diffusant des contenus audiovisuels ou musicaux.

Vecteur *: droit souple*

3.3.3. Organiser la répartition des rôles entre acteurs publics et acteurs privés dans la lutte contre les contenus illicites

Comme il a été vu dans la proposition n° 3, à la différence des hébergeurs de la législation actuelle, les plateformes ne seraient pas définies par leur rôle technique et passif mais par le fait qu'elles fournissent des services de référencement et de classement de contenus, biens ou services édités ou fournis par des tiers. Elles devraient cependant bénéficier, comme les hébergeurs, d'un régime de responsabilité civile et pénale limitée. En effet, les contenus, biens ou services ne sont pas définis ou fournis par les plateformes, mais par des tiers. Si la responsabilité des plateformes est définie de manière trop large, elles risquent de pratiquer une censure plus active, ce qui pourrait nuire à la liberté d'expression ou à la liberté d'entreprendre. Comme pour les hébergeurs, la responsabilité des plateformes ne devrait donc être engagée que si elles ont connaissance du caractère manifestement illicite des contenus[507], biens ou services proposés ou si, une fois cette connaissance acquise, elles n'ont pas agi promptement pour les retirer. Il ne devrait pas leur être imposé d'obligation générale de surveillance.

En revanche, des obligations de surveillance ciblée pourraient être instaurées pour les hébergeurs passifs comme pour les plateformes. Les dispositions du 3 de l'article 14 de la directive 2000/31 sur le commerce électronique prévoient la possibilité pour une juridiction ou une autorité administrative d'un État-membre d'enjoindre à un hébergeur de mettre un terme à une violation ou de prévenir une violation. D'ores et déjà, les juridictions françaises peuvent prononcer de telles injonctions, en particulier en référé dans le cadre de l'article L. 336-2 du code de la propriété intellectuelle. Un rapport remis à la ministre de la culture sur la lutte contre la contrefaçon en ligne[508] a préconisé de s'appuyer sur la faculté ouverte par la directive pour permettre à une autorité administrative de prononcer une « *obligation de retrait prolongé* » consistant, pour un prestataire de service de communication au public en ligne, à empêcher pendant une durée déterminée la réapparition d'un contenu précis.

De telles injonctions ne sont possibles qu'à la condition de ne pas constituer une « *obligation générale de surveillance* », prohibée par l'article 15 de la directive. La jurisprudence européenne (arrêt *SABAM c. Netlog NV*, 16 février 2012, C260/10)

507. Conformément à la réserve d'interprétation formulée par le Conseil constitutionnel dans sa décision n° 2004-496 DC du 10 juin 2004, § 9.

508. Mireille Imbert-Quaretta, *Outils opérationnels de prévention et de lutte contre la contrefaçon en ligne*, mai 2014.

comme nationale (arrêts du 12 juillet 2012 de la Cour de cassation précités) est venu rappeler cette limite : toute injonction qui s'apparenterait, par ses effets, à une obligation générale de surveillance est proscrite par la directive. L'obligation mise à la charge de l'hébergeur ou de la plateforme doit donc être strictement proportionnée, limitée dans le temps, ciblée sur des contenus précis, et mise en œuvre de façon à ne pas constituer une « *surveillance généralisée* ». Il existe ainsi une voie médiane, mentionnée par la directive elle-même, entre la répétition des notifications de retrait à chaque fois que le contenu réapparaît sur un site et l'obligation générale de surveiller les contenus du site.

Le système d'obligation de retrait prolongé sur injonction de l'autorité administrative devrait être prévu par la loi. Au-delà des seules violations de la propriété littéraire et artistique, il pourrait également concerner les atteintes au droit des marques et la vente de biens ou de services illicites. Les destinataires des injonctions pourraient exercer les voies de recours de droit commun devant la juridiction administrative.

Proposition n° 28 : Aligner le régime de responsabilité civile et pénale des plateformes sur celui des hébergeurs. Prévoir une obligation pour les hébergeurs et les plateformes d'empêcher, durant un délai déterminé, la réapparition des contenus ayant fait précédemment l'objet de retrait. Cette obligation serait prononcée par l'autorité administrative.

Vecteur *: loi (pour les plateformes, après l'intervention de la directive de l'Union européenne créant la catégorie juridique des plateformes).*

Les plateformes développent depuis plusieurs années des outils de reconnaissance automatique des contenus illicites, notamment dans le cadre de la lutte contre la contrefaçon (cf. *supra* 2.3.1). Ces outils s'avèrent efficaces dans la lutte contre les contenus illicites. Ils soulèvent cependant des questions quant à leur effet sur l'exercice de la liberté d'expression, notamment en raison des risques de « *surblocage* », c'est-à-dire de retrait de contenus en réalité licites ; tant la CJUE que la CEDH ont montré qu'elles étaient particulièrement attentives à la prévention de ces risques[509].

La voie préconisée ici consiste à admettre l'utilisation de ces outils, en raison de leur efficacité dans la lutte contre les contenus illicites, mais à l'encadrer davantage afin d'en limiter les risques pour la liberté d'expression. En premier lieu, les plateformes devraient être tenues, dans le prolongement de leur obligation générale de loyauté, à une obligation de transparence envers les utilisateurs sur la mise en œuvre de ces outils. En second lieu, la loi devrait prévoir expressément la nécessité de limiter au strict minimum les risques de surblocage. Les outils de reconnaissance automatique peuvent par exemple être peu aptes à distinguer une contrefaçon illicite d'une parodie couverte par l'exception au droit d'auteur prévue par le 4° de l'article L. 122-5 du code de la propriété intellectuelle. Les risques de surblocage n'apparaissent pas aujourd'hui d'une ampleur suffisante pour justifier un

509. Cf. CJUE, 27 mars 2014, *Telekabel*, C-314/12 et CEDH 18 décembre 2012, *Yildirim c. Turquie*, n° 3111/10.

contrôle administratif *a priori* des outils de surveillance. Toutefois, les plateformes devraient, dans le cadre de leur obligation de transparence, rendre compte chaque année d'une part des précautions prises pour limiter le surblocage, d'autre part du nombre de contenus retirés par application des outils de surveillance.

Proposition n° 29 : Encadrer l'utilisation des outils de surveillance automatique des contenus mis en œuvre volontairement par les plateformes en prévoyant une obligation de transparence sur l'utilisation de ces outils, leur fonctionnement et l'étendue des blocages de contenus qu'ils entraînent.

Vecteur *: loi (après l'intervention de la directive de l'Union européenne créant la catégorie juridique des plateformes).*

3.3.4. Adapter les instruments de la promotion du pluralisme des médias

L'existence de modalités spécifiques de contrôle des concentrations, qui complètent le contrôle général opéré par l'Autorité de la concurrence, est une garantie importante du pluralisme des médias. Le Conseil constitutionnel a censuré à deux reprises des lois qui prévoyaient en la matière des dispositions insuffisamment précises et effectives, au motif qu'elles privaient de protection légale une exigence constitutionnelle[510]. Le contrôle de la concentration dans les médias n'est d'ailleurs pas propre à la France et existe selon des modalités diverses dans la plupart des grandes démocraties[511].

L'article 11 de la loi du 1er août 1986 portant réforme du régime juridique de la presse interdit à un même groupe de contrôler des quotidiens d'information politique et générale représentant plus de 30 % de la diffusion imprimée nationale. Dans le domaine de l'audiovisuel, la loi du 30 septembre 1986 comporte plusieurs séries de dispositions. Celles-ci restreignent tant la part du capital qu'une seule personne peut détenir dans une société de télévision diffusant par voie hertzienne[512] que le nombre de services de télévision et de radio qui peuvent être détenus par une même personne[513]. Pour les concentrations dites « *pluri-médias* », tendant à la constitution de groupes exerçant leur activité sur plusieurs types de médias,

510. Décision n° 86-2010 DC du 29 juillet 1986, *Loi portant réforme du régime juridique de la presse*, § 20 à 24 ; décision n° 86-217 DC du 18 septembre 1986, *Loi relative à la liberté de communication*, § 25 à 37.

511. Cf. *Les problèmes de concentration dans le domaine des médias*, rapport au Premier ministre de la commission instituée par le décret n° 2005-217 du 8 mars 2005, décembre 2005.

512. L'article 39 de la loi limite cette part à 49 % pour les sociétés dont l'audience dépasse 8 %.

513. Pour la radio, l'article 41 ne permet à une même personne d'être titulaire, directement ou indirectement, de plusieurs autorisations de diffusion de services de radio que si la somme des populations desservies ne dépasse pas 150 millions de personnes. Pour la télévision, le même article ne permet pas à une même personne d'être titulaire de plus de sept autorisations pour la diffusion en TNT.

l'article 41-1 et 41-1-1 de la loi fixent une règle dite de « *deux sur trois* » : aucune autorisation de diffusion nationale de services de télévision ou de radio par voie hertzienne ne peut être délivrée si elle met son titulaire en position de dépasser des seuils d'influence dans plus de deux médias parmi la télévision, la radio et la presse écrite, la définition de ces seuils d'influence reposant sur des modalités spécifiques pour chaque média[514].

L'objectif assigné par le Conseil constitutionnel au contrôle des concentrations dans les médias, qui consiste selon ses termes à ce que les destinataires des médias « *soient à même d'exercer leur libre choix sans que ni les intérêts privés ni les pouvoirs publics puissent y substituer leurs propres décisions ni qu'on puisse en faire les objets d'un marché* », conserve toute sa pertinence. Cependant, dans un univers marqué par la surabondance des contenus, les principales menaces pesant sur le libre choix des destinataires ne tiennent plus seulement à une concentration excessive, mais aussi à la fragilisation du modèle économique de la presse, alors que celle-ci demeure une source essentielle d'information de qualité.

Les dispositions actuelles présentent plusieurs lacunes, dont certaines avaient déjà été soulignées en 2005 par le rapport de la commission présidée par Alain Lancelot[515], d'autres étant liées aux transformations du secteur causées par le numérique :

- En matière de presse, la définition des seuils de diffusion ne prend en compte que la diffusion imprimée, alors que la part de celle-ci est en constant recul au profit de la diffusion numérique. Même si l'évaluation de la diffusion numérique est plus complexe, son exclusion prive aujourd'hui la définition du seuil d'une grande part de sa pertinence.

- De manière générale, l'ensemble des dispositions relatives au contrôle des concentrations dans les médias s'attachent à un mode technologique particulier de diffusion, en distinguant par exemple la diffusion analogique de la diffusion numérique. Cela implique leur adaptation fréquente, ce qui est source de complexité. En outre, l'on peut s'interroger sur la pertinence de cette approche par technologie au regard de l'objectif de pluralisme dans les médias.

- Les dispositions actuelles ne s'intéressent qu'au contrôle des éditeurs de médias. Elles ne permettent pas de prendre en compte le rôle croissant de prescription joué par les distributeurs et les plateformes ; ainsi, une part très significative des consultations de sites d'information est aujourd'hui engendrée par leur référencement par des moteurs de recherche généralistes ou spécialisés, par des agrégateurs ou, de plus en plus, par les réseaux sociaux.

- Enfin, l'on peut s'interroger sur la définition des seuils en matière de concentration « *pluri-médias* ». Comme le relevait le rapport de la commission présidée par Alain Lancelot, les groupes pluri-médias sont peu développés en France comparé aux

514. Pour la télévision et la radio, être titulaire d'autorisations couvrant respectivement plus de 4 et plus de 30 millions de personnes ; pour la presse écrite quotidienne d'information politique et générale, éditer ou contrôler des quotidiens représentant plus de 20 % de la diffusion nationale.

515. *Les problèmes de concentration dans le domaine des médias*, op. cit.

autres pays européens, même s'il n'est pas avéré que les dispositions présentées ci-dessus soient responsables de cette situation. S'il convient de veiller à éviter la constitution de groupes trop influents, leur développement peut dans certains cas servir le pluralisme s'il permet de renforcer des titres de presse écrite, dont on connaît les difficultés financières et qui ont besoin de ressources pour investir, notamment pour faire face au nouvel environnement numérique.

Guidée par l'objectif de valeur constitutionnelle de pluralisme des courants d'opinion, une réforme du régime de concentration des médias, portant notamment sur les quotas de diffusion et la mesure des bassins d'audience utilisés pour la limiter, est souhaitable pour reconnaître l'existence de modes de diffusion de plus en plus diversifiés.

Proposition n° 30 : Revoir le contrôle de la concentration dans les médias, et notamment les quotas de diffusion et la mesure des bassins d'audience utilisés pour la limiter, afin de mieux garantir le pluralisme au regard de l'ensemble des modes de diffusion contemporains.

Vecteur *: concertation en vue d'une loi.*

3.3.5. Développer la médiation pour régler les litiges liés à l'utilisation des technologies numériques

Nombre de litiges liés à l'utilisation des technologies numériques, qu'il s'agisse de contestations relatives aux données personnelles, aux atteintes à la réputation sur internet ou au retrait de contenus mis en ligne, peuvent être qualifiés de « *petits litiges* » : leurs enjeux sont parfois significatifs pour les personnes concernées mais les intérêts pécuniaires en cause sont le plus souvent limités. En consacrant le droit au déréférencement, l'arrêt *Google Spain* du 13 mai 2014 de la CJUE a sans doute créé une nouvelle source de petits litiges, puisqu'il reviendra aux moteurs de recherche de procéder dans chaque cas à une balance des intérêts, qui pourra être contestée par les parties en présence. Les procédures juridictionnelles classiques sont peu adaptées au traitement de ces petits litiges, ce qui conduit nombre de personnes à renoncer à faire valoir leurs droits. La création de l'action collective en matière de protection des données personnelles (cf. proposition n° 9) constitue une première réponse à cette difficulté. Une seconde réponse, qui concerne quant à elle l'ensemble des litiges évoqués ci-dessus, consiste à développer la médiation.

Pour que le système de médiation mis en place soit accessible, il doit être facile d'accès, peu onéreux et proposer dans des délais rapides une solution aux cas qui lui sont soumis. Les échanges entre les parties devraient être conduits de manière largement dématérialisée. Le recours à la médiation serait purement volontaire et ne serait pas une condition préalable du recours au juge ou à la CNIL. Conformément aux règles de droit commun (article 2238 du code civil), le recours à la médiation suspendrait la prescription.

Ce dispositif de médiation devrait être confié à une structure *ad hoc*. Les dépenses correspondantes seraient mises à la charge des personnes y recourant[516] . En Corée du sud, une autorité administrative indépendante spécifique a été créée pour gérer la médiation en matière de protection des données personnelles[517] : elle est composée de fonctionnaires ayant une expérience en matière de données personnelles, de juristes qualifiés, d'hommes d'affaires et de représentants des entreprises du secteur des technologies numériques, de chercheurs et de représentants d'associations de protection des consommateurs. En droit français, le recours à un groupement d'intérêt public ou à une association permettrait d'éviter la création d'une AAI supplémentaire. La structure de médiation devrait en tout état de cause avoir une composition analogue, associant plusieurs formes d'expertises et des représentants des différentes parties prenantes. Les solutions proposées aux parties devraient être adoptées par des formations collégiales.

Un tel système de médiation pourrait être créé sans intervention du législateur, par accord entre les différentes parties prenantes. L'intervention du législateur serait cependant nécessaire en l'absence d'accord volontaire ou si le recours à la formule de l'AAI devait être retenu.

Proposition n° 31 : Mettre en place un système de médiation facilement accessible pour régler les petits litiges entre personnes privées liés à l'utilisation des technologies numériques, tels que ceux concernant les données personnelles, les atteintes à la réputation sur internet ou le retrait de contenus mis en ligne.

Vecteur *: accord entre les parties prenantes ou loi.*

3.4. Assurer le respect des droits fondamentaux dans l'utilisation du numérique par les personnes publiques

3.4.1. Poursuivre l'ouverture des données publiques tout en prévenant les risques pour la vie privée

Renforcer la dynamique de mise en ligne progressive des données publiques

L'ouverture des données publiques, ou « *Open Data* », fait l'objet depuis 2011 d'une politique volontariste du gouvernement, mise en œuvre sous l'impulsion d'un service dédié rattaché aux services du Premier ministre, la mission Etalab.

516. Le financement pourrait être complété le cas échéant par un transfert de crédits en provenance des ou de l'autorité de contrôle correspondant aux économies faites par celle(s)-ci du fait de ce nouveau dispositif.

517. Il s'agit du PICO, que l'on peut traduire par « *comité de médiation des conflits relatifs aux informations personnelles* ».

Le « *vademecum sur l'ouverture et le partage des données publiques* » du 17 septembre 2013, adressé par le Premier ministre aux ministres, prévoit que « *toutes les données produites ou détenues par l'administration qui entrent dans le champ des données publiques doivent être partagées, gratuitement, et librement réutilisables* ». Sur le plan international, la France a participé à l'adoption d'un instrument de droit souple, la « *Charte du G8 pour l'ouverture des données publiques* » du 18 juin 2013, qui énonce un principe « *d'ouverture par défaut* » ; conformément à cette charte, elle a adopté le 6 novembre 2013 un plan d'action définissant ses priorités.

Ce volontarisme politique, qui se traduit par l'affichage d'un principe d'ouverture par défaut aujourd'hui inscrit dans un instrument de droit souple, contraste avec la faiblesse des obligations prévues par le droit dur. La loi du 17 juillet 1978 consacre deux droits : le droit d'accès aux documents administratifs, et depuis l'ordonnance du 6 juin 2005 ayant transposé la directive n° 2003/98/CE[518], le droit de réutilisation des informations publiques. Elle ne prévoit pas en revanche d'obligation générale de mise en ligne : son article 7 n'impose de publier que « *les directives, les instructions, les circulaires, ainsi que les notes et réponses ministérielles qui comportent une interprétation du droit positif ou une description des procédures administratives* » ; pour tous les autres documents administratifs, la publication n'est qu'une faculté. Ce décalage a été relevé par une mission d'information du Sénat, qui a préconisé d'inscrire dans la loi une obligation de mise en ligne progressive de l'ensemble des bases de données détenues par l'administration[519].

L'écriture dans la loi d'une telle obligation pourrait présenter plusieurs avantages. Tout d'abord, elle donnerait une portée plus forte au mouvement d'ouverture des données publiques, qui ne repose aujourd'hui que sur une décision du Premier ministre et qui pourrait être remis en cause par un acte de la même autorité[520]. Dès lors qu'un droit à la mise en ligne des données publiques serait reconnu aux citoyens, la mesure entrerait bien dans le domaine de la loi défini par la Constitution[521]. En outre, le Gouvernement ne peut décider que de l'ouverture des données publiques détenues par l'État et, dans une certaine mesure, de celles détenues par ses opérateurs ; la loi permettrait d'imposer des obligations aux collectivités territoriales, qui détiennent des données publiques d'un intérêt majeur

518. Directive n° 2003/98/CE du 17 novembre 2003 concernant la réutilisation des informations du secteur public, dite « *directive ISP* ».

519. G. Gorce et F. Pillet, *Mission d'information du Sénat sur l'*open data *et la vie privée*, avril 2014.

520. Rien n'interdirait par exemple à l'État de fermer la plateforme data.gouv.fr qui sert à la mise en ligne des données publiques.

521. Si l'on considère que le droit d'accès aux documents administratifs est une liberté publique au sens de l'article 34 de la Constitution, alors la mise en ligne de ces documents est une garantie fondamentale pour l'exercice de cette liberté et entre bien dans le domaine de la loi. Plaide pour cette reconnaissance le fait qu'au niveau de l'Union européenne, le droit d'accès aux documents est consacré par l'article 42 de la Charte des droits fondamentaux. On peut également relever que la définition d'une obligation générale d'ouverture des données publiques reviendrait à étendre le champ des documents administratifs soumis à une obligation de publication, défini par l'article 7 de la loi du 17 juillet 1978, et imposerait donc de modifier la loi.

pour l'activité économique et le débat démocratique. Si certaines collectivités territoriales ont devancé l'État dans l'ouverture des données publiques, leur action en la matière reste aujourd'hui inégale.

Toutefois, la définition d'une telle obligation générale se heurte à plusieurs objections. Tout d'abord, le travail de recensement et de constitution par l'administration des jeux de données à publier, initié récemment, est encore loin d'être achevé. La charte du G8 reconnaît à ce sujet que la préparation de données de qualité prend du temps et qu'il est nécessaire de consulter les parties prenantes pour identifier les jeux de données à publier en priorité. Ensuite, l'appropriation de l'*Open Data* par les acteurs économiques et sociaux n'en est encore qu'à ses débuts : dans cette phase d'initiation, la mise en ligne prioritaire de jeux de données sélectionnés pour leur « *fort potentiel* »[522] est sans doute plus propice à la compréhension des enjeux de l'*Open Data* que la publication d'une masse d'informations de valeur inégale. Enfin, une telle obligation générale représenterait une charge non négligeable pour les collectivités territoriales, dans une période de diminution programmée de leurs ressources.

Somme toute, la voie du droit souple apparaît plus appropriée pour promouvoir le développement de l'*Open Data*, notamment auprès des collectivités territoriales. Une charte d'engagements et de bonnes pratiques pourrait être élaborée par l'État, les associations de collectivités territoriales et des représentants des utilisateurs des données (associations engagées dans l'ouverture des données publiques, et entreprises). Cette charte engagerait chaque organisme public adhérent à définir un programme d'ouverture de ses données publiques, à respecter des standards de qualité et à veiller à limiter les risques de réidentification. En outre, le rôle d'appui des services de l'État aux collectivités territoriales souhaitant ouvrir leurs données publiques pourrait être accru[523]. Le décret relatif au secrétariat général pour la modernisation de l'action publique (SGMAP), auquel est rattachée la mission Etalab, pourrait être modifié pour lui confier expressément ce rôle.

Proposition n° 32 : Afin de promouvoir le développement de l'*open data* auprès des personnes publiques, notamment les collectivités territoriales :

- Adopter une charte d'engagements et de bonnes pratiques signée par l'État, les associations de collectivités territoriales et les représentants des utilisateurs des données publiques, et promouvoir l'adhésion des personnes publiques à cette charte.

- Accroître le rôle d'appui des services de l'État aux collectivités territoriales souhaitant ouvrir leurs données publiques

Vecteur *: droit souple (charte d'engagements et de bonnes pratiques) et décret.*

522. Selon l'expression employée par le plan d'action présenté par la France dans le cadre de la charte du G8.

523. À ce jour, le décret n° 2012-1198 du 30 octobre 2012 portant création du secrétariat général pour la modernisation de l'action publique prévoit seulement que le portail www.data.gouv.fr est ouvert aux collectivités territoriales qui souhaitent l'utiliser.

Une large part des données publiques ne présente aucun lien avec des données personnelles. C'est le cas de nombre des jeux de données présentés comme « *les plus populaires* » sur la plateforme www.data.gouv.fr : la liste des immeubles protégés au titre des monuments historiques, les indicateurs de « *valeur ajoutée* » des lycées d'enseignement général ou technologique, le tableau de bord des déchets ou encore les données d'observation des principales stations météorologiques. Pour autant, les administrations gèrent aussi, bien sûr, un grand nombre de bases de données concernant des individus[524]. La question de la compatibilité entre la politique d'ouverture des données publiques et la protection des données personnelles est donc susceptible de se poser à chaque administration.

La législation y apporte une réponse claire sur le plan des principes. L'article 7 de la loi du 17 juillet 1978 subordonne la publication à la mise en œuvre d'un traitement rendant « *impossible* » l'identification des personnes. L'article 13 n'autorise la réutilisation des informations publiques contenant des données personnelles que si la personne intéressée y a consenti, si l'autorité détentrice est en mesure de les rendre anonymes ou si une disposition législative ou réglementaire le permet ; le réutilisateur doit en tout état de cause respecter la loi du 6 janvier 1978. Sauf exception prévue par la loi, ces dispositions conduisent donc les administrations envisageant de mettre en ligne une base de données contenant des données personnelles à les anonymiser.

Sur le plan pratique, la question de savoir ce qu'est une anonymisation satisfaisante est en revanche plus délicate. Le fait de supprimer les identifiants de la personne tels que son nom ou son NIR en les remplaçant par un numéro aléatoire n'est pas suffisant, car la personne peut être identifiée grâce aux autres informations contenues à son sujet dans la base ; selon les termes employés par le G29 dans un avis du 10 avril 2014, la « *pseudonymisation* » ne suffit pas à assurer « *l'anonymisation* »[525]. Ainsi, une étude française a montré que 89 % des patients ayant fait un séjour à l'hôpital au cours d'une année pouvaient être identifiés à partir des seules informations suivantes : l'hôpital d'accueil, le code postal du domicile, le mois et l'année de naissance, le sexe, le mois de sortie et la durée du séjour[526]. Selon une autre étude, plus de 80 % des Américains peuvent être identifiés par la combinaison de leur code postal, de leur sexe et de leur date de naissance[527]. De

524. Un des jeux de données les plus populaires sur le site www.data.gouv.fr, les aides perçues par chaque bénéficiaire au titre de la politique agricole commune (PAC), a d'ailleurs vu sa base juridique partiellement invalidée par la CJUE pour méconnaissance du droit à la protection des données personnelles : celle-ci a jugé que les règlements de l'Union européenne qui imposaient la publication des sommes perçues par chaque bénéficiaire portaient une atteinte disproportionnée à ce droit, en ce qui concerne les aides perçues par les personnes physiques (CJUE, Gde Ch., 9 novembre 2010, *Volcker und Markus Schecke GbR et Hartmut Eifert*, C-92/09 et C-93/09.

525. Article 29 Working Party, "Opinion 05/2014 on Anonymisation Techniques", 10 avril 2014, 0829/14/EN WP216.

526. Étude du docteur Dominique Blum, citée par P.-L. Bras et A. Loth, *op. cit*.

527. L. Sweeney, Weaving Technology and Policy Together to Maintain Confidentiality, *Journal of Law, Medicine &Ethics*, 25, nos. 2&3 (1997): 98-110

manière générale, les techniques de réidentification de données anonymisées ont connu au cours des dernières années d'importants progrès, conduisant à remettre en cause des procédés jusqu'alors considérés comme fiables. La multiplication des jeux de données accessibles en ligne associée à l'*Open Data* est susceptible d'accroître ces risques.

Deux recommandations peuvent être déduites de ces constats. Tout d'abord, les rapports d'experts les plus récents montrent que pour parvenir à un degré d'anonymisation satisfaisant, il faut recourir à une combinaison complexe de plusieurs techniques (agrégation, « *floutage* »[528], introduction d'erreurs aléatoires...). La plupart des responsables d'administration, appelés à décider de la mise en ligne des jeux de données, ne disposent pas en interne d'une expertise suffisante pour mettre en œuvre ces techniques de manière adéquate. L'État doit donc définir une organisation permettant de s'assurer, préalablement à toute mise en ligne, que les bonnes pratiques d'anonymisation ont été mises en œuvre. Ces standards pourraient être définis par la CNIL, en concertation étroite avec le comité du secret statistique[529] et la CADA[530]. Chaque ministère devrait constituer en son sein un pôle d'expertise destiné à appuyer ses administrations dans la mise en œuvre des procédés d'anonymisation. Les services statistiques ministériels apparaissent les mieux placés pour constituer ces pôles d'expertise. Ces services d'expertise pourraient être accessibles gratuitement aux collectivités territoriales qui en font la demande auprès du préfet[531].

En second lieu, lorsqu'un risque significatif de réidentification ne peut être écarté, des alternatives à la mise en ligne doivent être envisagées pour mieux concilier accès aux données publiques et protection des données personnelles. Cela doit être en particulier le cas lorsque sont en cause des données sensibles comme les données de santé, les données fiscales ou les informations sur les difficultés sociales des personnes. L'accès à la base de données complète peut être subordonné à une

528. Il s'agit par exemple de remplacer la date par l'année de naissance ou le code postal par le numéro du département.

529. Prévu par l'article 6 *bis* de la loi du 7 juin 1951 sur l'obligation, la coordination et le secret en matière de statistiques, le comité du secret statistique « *est appelé à se prononcer sur toute question relative au secret en matière de statistiques* ». Il donne notamment son avis sur les demandes de communication des renseignements individuels issus des enquêtes de la statistique publique.

530. Le Memento intitulé *La protection des informations à caractère personnel dans le cadre de l'ouverture et du partage des données publiques*, établi par le Conseil d'orientation de l'édition publique et de l'information administrative (COEPIA) en juillet 2013, donne des indications générales mais pas les précisions techniques détaillées qui auraient vocation à figurer dans ces bonnes pratiques.

531. Une telle offre de services ne serait contraire ni à la liberté du commerce et de l'industrie, ni au droit de la concurrence. À l'exemple de la mission d'appui à la réalisation des contrats de partenariat, dont la création a été admise par le Conseil d'État (CE, Ass., 31 mai 2006, *Ordre des avocats au barreau de Paris*, n° 275531, Rec. p. 272), la fourniture d'un tel service entrerait dans la mission d'intérêt général, qui relève de l'État, de s'assurer du respect de la légalité par les personnes publiques.

autorisation, permettant de s'assurer du motif de la démarche, de la nécessité de l'accès aux données par rapport aux finalités poursuivies et des garanties présentées par le demandeur ; les données peuvent alors être communiquées selon des modalités faisant obstacle à leur dissémination[532]. Le cas échéant, il est possible de combiner mise en ligne de jeux de données agrégées et accès sur autorisation aux données détaillées. Cette approche, dite de « *protection différentielle de la vie privée* » (« *differential privacy* »), est préconisée de manière générale par le G29 ; les préconisations formulées récemment au sujet des données publiques de santé s'inscrivent également dans cette démarche[533].

Proposition n° 33 : Pour les données publiques comportant des données personnelles, maîtriser les conditions de leur ouverture afin de limiter étroitement le risque de réidentification. À cette fin :

- Faire définir par la CNIL, en concertation étroite avec le comité du secret statistique et la CADA, des standards d'anonymisation ;

- Constituer au sein de chaque ministère un pôle d'expertise en matière d'anonymisation, *a priori* au sein du service statistique ministériel ;

- Assurer l'accessibilité de ces services d'expertise aux collectivités territoriales qui en font la demande auprès du préfet.

- Lorsque le risque de réidentification ne peut être écarté, définir une procédure d'accès sur autorisation plutôt que de mettre en ligne, en particulier lorsque sont en cause des données sensibles (par exemple des données de santé, des données fiscales ou des informations sur les difficultés sociales des personnes).

Vecteur *: Droit souple (recommandations de bonnes pratiques) et organisation des services de l'État. Le cas échéant, dispositions législatives pour définir les procédures d'accès sur autorisation.*

3.4.2. Renforcer les garanties entourant l'usage des fichiers de police judiciaire

Les fichiers de police judiciaire ont connu une forte expansion au cours des quinze dernières années (cf. *supra* 1.3.3), liée notamment à l'allongement de la liste des infractions donnant lieu à enregistrement. Sans remettre en cause leur utilité pour les services de police, il apparaît souhaitable de renforcer à certains égards les garanties entourant leur utilisation et de corriger certaines fragilités juridiques, tout en définissant un régime d'expérimentation allégé pour la création de nouveaux fichiers.

532. Ainsi, il existe depuis 2009 au sein des services de la statistique publique un « *centre d'accès sécurisé distant aux données* » (CASD), qui permet de donner à des équipes de chercheurs ayant bénéficié d'une autorisation un accès à des données individuelles détaillées, sans que ces équipes aient la possibilité de conserver et de reproduire les données utilisées.
533. P.-L. Bras et A. Loth, *op. cit.*, et rapport de la commission sur l'*Open Data* en matière de santé [à paraître].

Mieux tirer les conséquences des décisions judiciaires

Dans un arrêt du 18 avril 2013 (*M.K. c/ France*, n° 19522/09), la CEDH a condamné la France en raison des règles relatives au fichier automatisé des empreintes digitales (FAED). Elle a jugé qu'il avait été porté une atteinte disproportionnée au droit à la vie privée du requérant, au motif que le décret relatif au FAED n'opérait « *aucune distinction fondée sur l'existence ou non d'une condamnation par un tribunal, voire même d'une poursuite par le ministère public* » (§ 42). En l'espèce, le requérant avait bénéficié d'une relaxe dans une première affaire et d'un classement sans suite dans une seconde, les deux affaires concernant des vols de livres. Les articles 7 et 7-1 du décret n°87-249 du 8 avril 1987 relatif au fichier automatisé des empreintes digitales géré par le ministère de l'intérieur disposent que les données peuvent être effacées par le procureur de la République, d'office ou à la demande de l'intéressé, lorsque leur conservation n'apparaît plus nécessaire compte tenu de la finalité du fichier. Le décret ne fixe en revanche aucun mécanisme contraignant de prise en compte des décisions judiciaires, ce qui a entraîné la condamnation de la France par la CEDH.

La conservation dans un fichier de police d'informations relatives à des personnes mises en cause mais n'ayant pas fait l'objet d'une condamnation devenue définitive n'apparaît pas, par elle-même, mise en question dans l'arrêt de la CEDH. Son principe a d'ailleurs été admis par le Conseil constitutionnel (décision n° 2003-467 DC du 13 mars 2003, *Loi pour la sécurité intérieure*, § 40) et par le Conseil d'État (CE 11 avril 2014, *Ligue des droits de l'homme*, n° 360759, à mentionner aux tables). En revanche, les textes autorisant le fichier devraient définir précisément les conséquences à tirer des décisions judiciaires concernant la personne mise en cause, comme c'est le cas pour le fichier « *Traitements d'antécédents judiciaires* » (TAJ). Selon l'article 230-8 du code de procédure pénale, en cas de décision de relaxe ou d'acquittement devenue définitive, les données concernant la personne mise en cause sont effacées, sauf si le procureur de la République en décide le maintien pour des raisons liées aux finalités du fichier. En cas de non-lieu ou de classement sans suite, les données font l'objet d'une mention qui en interdit l'accès dans le cadre des enquêtes administratives, sauf si le procureur de la République en décide l'effacement.

Cette dernière disposition est sans objet pour le FAED, qui ne peut être utilisé pour les enquêtes administratives. En revanche, les autres dispositions prévues pour le TAJ pourraient être transposées au FAED, ce qui répondrait aux reproches formulés par la CEDH. Le fichier national automatisé des empreintes génétiques (FNAEG), dont les dispositions sont rédigées dans des termes identiques à celles du FAED[534], devrait faire l'objet du même ajustement.

534. Article 706-54 du code de procédure pénale : « (…) *Ces empreintes sont effacées sur instruction du procureur de la République agissant soit d'office, soit à la demande de l'intéressé, lorsque leur conservation n'apparaît plus nécessaire compte tenu de la finalité du fichier.* (…) »

Proposition n° 34 : Préciser, en s'inspirant des dispositions relatives au fichier « *Traitements d'antécédents judiciaires* » (TAJ), les conséquences à tirer des décisions judiciaires (classement sans suite, non-lieu, relaxe et acquittement) quant à l'effacement des données relatives aux personnes mises en cause, pour le fichier automatisé des empreintes digitales (FAED) et le fichier national automatisé des empreintes génétiques (FNAEG).

Vecteur *: décret pour le FAED, loi pour le FNAEG.*

Les dispositions législatives et réglementaires relatives au TAJ n'encourent pas les mêmes reproches. En revanche, les rapports de contrôle rendus publics par la CNIL en 2009 et en 2013 sur le TAJ et ses prédécesseurs (système de traitement des infractions constatées (STIC) pour la police nationale, JUDEX pour la gendarmerie nationale) ont montré d'importantes difficultés dans la mise en œuvre effective de ces dispositions[535]. En 2007, les taux de prise en compte des décisions de classement sans suite, de non-lieu, d'acquittement et de relaxe n'étaient respectivement que de 21,5 %, 0,5 %, 6,9 % et 31,2 % ; le rapport de 2013 ne fait pas état d'améliorations significatives sur ce point. À l'avenir, l'interconnexion du fichier CASSIOPEE du ministère de la justice et du fichier TAJ devrait lever ces difficultés en permettant la transmission automatique des suites judiciaires. Elle ne permettra cependant pas la correction des erreurs pour le « *stock* » des fiches antérieures à l'interconnexion, qui concerne un très grand nombre de personnes[536], dont les données sont appelées à être conservées pour une longue durée[537]. Ceci pose d'autant plus de problèmes qu'en vertu des articles L. 114-1 et L. 234-1 du code de la sécurité intérieure, les informations contenues dans le TAJ sont utilisées dans un très grand nombre d'enquêtes administratives, plus d'un million d'emplois étant concernés[538].

535. CNIL, *Conclusions du contrôle du système de traitement des infractions constatées (STIC)*, janvier 2009 ; CNIL, *Conclusions du contrôle des fichiers d'antécédents du ministère de l'intérieur*, juin 2013 ; cf. aussi les conclusions convergentes de D. Batho et J.-A. Bénisti, *Rapport d'information de l'Assemblée nationale sur les fichiers de police*, mars 2009.

536. Selon le rapport de 2013 de la CNIL, le fichier TAJ comporte 12,2 millions de fiches relatives à des personnes mises en cause, mais il peut comporter des « *doubles comptes* » en raison du caractère récent de la fusion entre le STIC et JUDEX : une même personne peut être présente dans plusieurs fiches.

537. Selon l'article R. 40-27, la durée de conservation normale pour une personne majeure mise en cause est de vingt ans ; elle est de quarante ans pour les infractions les plus graves et de 5 ans pour les infractions les moins graves. Pour une personne mineure mise en cause, la durée de conservation normale est de 5 ans et dix ou 20 ans pour les infractions les plus graves.

538. Les articles R. 114-2 à R. 114-5 du code de la sécurité intérieure définissent la liste des procédures administratives dans le cadre desquelles il est possible de consulter le TAJ ; elles concernent notamment les emplois suivants : emplois impliquant l'accès ou le convoyage d'informations ou de supports protégés au titre du secret de la défense nationale, activités privées de sécurité (gardiennage, transport de fonds, recherche privée, etc.), services internes de sécurité de la SNCF et de la RATP, membres des juridictions administratives et judiciaires, militaires, agents de la police nationale et des douanes, agents de la police municipale, professions liées aux jeux de hasard, etc.

La correction du « *stock* » des fiches du TAJ représente sans nul doute un effort important pour les services concernés. Elle est cependant nécessaire au respect des droits des personnes et tout en étant dans l'intérêt des services. Elle est requise pour mettre en conformité le TAJ avec le 5° de l'article 6 de la loi du 6 janvier 1978, qui dispose que les données personnelles traitées doivent être « *exactes, complètes et, si nécessaire, mises à jour* » et que « *les mesures appropriées doivent être prises pour que les données inexactes ou incomplètes au regard des finalités pour lesquelles elles sont collectées ou traitées soient effacées ou rectifiées* »[539]. Le ministère de l'intérieur devrait donc définir un plan d'apurement du stock, au besoin étalé sur plusieurs années, afin de parvenir à une situation dans laquelle l'ensemble des fiches ont été vérifiées.

Proposition n° 35 : Définir un plan d'apurement des erreurs et insuffisances du fichier « *Traitements d'antécédents judiciaires* » (TAJ), notamment sur les suites judiciaires données aux mises en cause, afin de mettre à jour l'ensemble des fiches qui y sont contenues.

Vecteur *: action du ministère de la justice et du ministère de l'intérieur.*

Mettre en œuvre la décision du Conseil constitutionnel concernant le FNAEG

Dans sa décision n° 2010-25 QPC du 16 septembre 2010, le Conseil constitutionnel a déclaré conformes à la Constitution les dispositions législatives relatives au FNAEG. Il a toutefois formulé une réserve d'interprétation à l'attention du pouvoir réglementaire, qui détermine la durée de conservation des données : selon ses termes, « *il appartient au pouvoir réglementaire de proportionner la durée de conservation de ces données personnelles, compte tenu de l'objet du fichier, à la nature ou à la gravité des infractions concernées tout en adaptant ces modalités aux spécificités de la délinquance des mineurs* » (§ 18).

À ce jour, le pouvoir réglementaire n'a pas tiré les conséquences de cette décision, la dernière modification des dispositions réglementaires relatives au FNAEG étant intervenue le 8 juillet 2010. Selon l'article R. 53-14 du code de procédure pénale, la durée de conservation est de quarante ans, quelle que soit la nature de l'infraction et sans que soit prise en compte la minorité de la personne au moment de l'enregistrement. La durée de conservation est donc la même pour des actes de barbarie commis par une personne majeure et pour des vols commis par une personne mineure.

539. La proposition de directive relative à la protection des personnes physiques à l'égard du traitement de données à caractère personnel par les autorités compétentes à des fins de prévention et de détection d'infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données, prévoit de manière encore plus nette que «*toutes les mesures raisonnables doivent être prises pour que les données inexactes, eu égard aux finalités pour lesquelles elles sont traitées soient effacées ou rectifiées sans délai*».

Les dispositions réglementaires relatives au FNAEG doivent donc être modifiées pour établir une échelle de durée en fonction de la gravité de l'infraction commise et pour tenir compte de la minorité de la personne au moment de l'enregistrement. Là encore, les dispositions relatives au TAJ peuvent servir de source d'inspiration.

Proposition n° 36 : Mettre en œuvre la décision n° 2010-25 QPC du 16 septembre 2010 du Conseil constitutionnel, en modulant la durée de conservation des données dans le fichier national automatisé des empreintes génétiques (FNAEG) en fonction de la gravité de l'infraction et de la minorité de la personne au moment de l'enregistrement.

Vecteur *: décret en Conseil d'État.*

Faciliter l'expérimentation de fichiers en matière de sécurité

Les articles 26 et 27 de la loi du 6 janvier 1978 subordonnent l'autorisation d'un fichier de police à un arrêté ministériel pris après avis de la CNIL ou à un décret en Conseil d'État pris après avis de la CNIL. En vertu de l'article 30 de la loi, les demandes d'avis à la CNIL doivent être accompagnées d'un dossier détaillé. En pratique, la conception technique doit être pleinement aboutie lorsque la demande d'avis est transmise à la CNIL, avant toute mise en œuvre du fichier en raison du régime d'autorisation préalable ; cela peut être difficile sur le plan opérationnel, les fichiers informatiques nécessitant souvent des phases de test et d'expérimentation pour corriger leurs dysfonctionnements. Comme l'ont proposé l'Assemblée nationale[540] et la CNIL, un régime d'expérimentation pourrait être prévu par la loi, qui permettrait à la CNIL de valider le traitement selon plusieurs étapes : d'abord au stade de l'expérimentation, où les exigences de spécification pourraient être allégées et où le traitement pourrait être mis en œuvre sur simple autorisation de la CNIL, dans le cadre de l'article 25 de la loi du 6 janvier 1978, puis au stade du déploiement généralisé. Au-delà des fichiers de police, le régime d'expérimentation pourrait concerner l'ensemble des traitements de données régis par les articles 26 et 27 de la loi[541].

Proposition n° 37 : Définir un régime d'autorisation aux formalités allégées (spécifications du traitement moins précises et autorisation délivrée par la CNIL dans le cadre de l'article 25 de la loi du 6 janvier 1978) pour les expérimentations de traitements de données régis par les articles 26 et 27 de la loi du 6 janvier 1978.

Vecteur *: loi.*

540. D. Batho et J.-A. Bénisti, *op. cit*.

541. Il s'agit des traitements qui intéressent la sûreté de l'État, la défense ou la sécurité publique, qui ont pour objet la prévention, la recherche, la constatation ou la poursuite des infractions pénales ou l'exécution des condamnations pénales ou des mesures de sûreté, qui portent sur des données parmi lesquelles figure le NIR ou qui portent sur des données biométriques nécessaires à l'authentification ou au contrôle de l'identité des personnes.

3.4.3. Conjuguer le plein respect des droits fondamentaux et l'efficacité de la surveillance des communications électroniques à des fins de prévention des atteintes à la sécurité nationale

Tirer les conséquences de l'arrêt Digital Rights Ireland *de la CJUE en matière d'accès et de durée conservation des métadonnées*

Quelle que soit l'interprétation à retenir de l'arrêt *Digital Rights Ireland* sur le principe de la conservation systématique des métadonnées (cf. *supra* 2.1.5), certaines conséquences de l'arrêt doivent d'ores et déjà être tirées en ce qui concerne l'accès aux métadonnées :

- L'accès aux métadonnées pour des finalités relevant de la police judiciaire devrait être réservé aux crimes et aux délits suffisamment graves. Celles-ci pourraient être définies en fonction du niveau de la peine maximale dont elles sont punies, ainsi que de leur fréquence et de l'importance du trouble causé à l'ordre public.

- Outre l'accès aux métadonnées à des fins de sécurité intérieure, dans le cadre des finalités définies par l'article L. 241-2 du code de la sécurité intérieure, ou à des fins de police judiciaire, certains organismes administratifs disposent de possibilités d'accès à des fins spécifiques. Il s'agit notamment de la HADOPI dans le cadre de la lutte contre la contrefaçon, de l'ANSSI à des fins de sécurité des systèmes d'information ou encore de l'administration fiscale et de l'Autorité des marchés financiers (AMF) pour tous les contrôles et enquêtes nécessités par leurs missions[542]. Compte tenu des termes de l'arrêt *Digital Rights Ireland*, qui ne retient comme finalité d'intérêt général justifiant l'accès aux métadonnées que la lutte contre la criminalité grave, il conviendrait de réexaminer ces régimes d'accès à des fins administratives et le cas échéant de restreindre les circonstances dans lesquelles cet accès peut être demandé ou les données qui peuvent être communiquées.

- La durée de conservation des données prévue par la législation française est aujourd'hui d'un an, sans distinction selon la gravité des infractions ou des menaces en cause, ce qui tombe sous le coup d'un des griefs retenus par la CJUE (§ 63 et 64). L'uniformité de la durée de conservation par les opérateurs ne peut être remise en cause dans le cadre d'un système de collecte systématique, car il n'est pas possible de déterminer dès la collecte l'usage qui sera fait de la donnée. En revanche, il serait possible de parvenir au même résultat en modulant la période accessible aux autorités concernées. La durée de conservation par les opérateurs demeurerait uniforme, mais pour certaines finalités, seules les données les plus récentes (par exemple celles d'une ancienneté de moins de trois mois ou de six mois) pourraient être communiquées.

542. L'accès de la HADOPI et de l'ANSSI est prévu par le III de l'article L. 34-1 du code des postes et des communications électroniques, celui de l'administration fiscale par les articles L 83 et L. 96 G du livre des procédures fiscales et celui de l'AMF par l'article L. 621-10 du code monétaire et financier.

- Enfin, il serait souhaitable d'apporter une protection particulière à certaines catégories de personnes dont les activités bénéficient d'un secret protégé par la loi : il s'agit notamment des avocats, des magistrats et des journalistes. Les parlementaires pourraient également bénéficier d'une protection en raison des immunités qui leur sont reconnues par la Constitution et de leur rôle de contrôle du gouvernement. Pour ces quatre catégories, les garanties prévues par le code de procédure pénale pour les interceptions judiciaires (interdiction de la retranscription des correspondances lorsqu'elle permet d'identifier une source, obligation d'information préalable du président de l'assemblée, du bâtonnier ou du président ou procureur général de la juridiction) devraient être étendues aux procédures d'accès aux métadonnées.

Proposition n° 38 : Tirer les conséquences de l'arrêt *Digital Rights Ireland* en ce qui concerne l'accès aux métadonnées, en :

- réservant l'accès à des fins de police judiciaire aux crimes et aux délits d'une gravité suffisante ;

- réexaminant les régimes prévoyant l'accès de certaines autorités administratives pour des finalités autres que la sécurité intérieure (par exemple HADOPI, ANSSI, administration fiscale, AMF), et notamment les circonstances dans lesquelles cet accès peut être demandé et les données peuvent être communiquées ;

- modulant la période accessible en fonction de la finalité et de la gravité des infractions ;

- étendant, pour l'accès aux métadonnées, les règles spécifiques de protection qui bénéficient aux parlementaires, aux avocats, aux magistrats et aux journalistes.

Vecteur *: loi.*

Préciser le cadre juridique de l'action des services de renseignement pour les interceptions opérées à l'étranger et l'utilisation de certains moyens d'investigation spéciaux

Les dispositions encadrant l'interception des communications ne s'appliquent qu'aux données entrant dans le champ de l'application de la loi française relative au secret des correspondances émises par la voie électronique, c'est-à-dire aux données traitées par les opérateurs soumis à l'obligation de déclaration préalable auprès de l'ARCEP prévue par l'article L. 33-1 du code des postes et des communications électroniques. En dehors de ce champ, l'action des services de renseignement est seulement soumise aux dispositions de l'article L. 241-3 du code de la sécurité intérieure, dont on a vu (cf. *supra* 2.1.5) qu'elles étaient obsolètes sur le plan technique, tout en ne répondant pas à l'exigence de prévisibilité de la loi formulée par la jurisprudence de la CEDH.

Comme il a déjà été exposé, l'interception des communications à l'étranger n'a pas à être entourée de garanties équivalentes à celles prévues dans le champ

d'application de la loi sur le secret des correspondances. Afin de satisfaire à l'exigence de prévisibilité de la loi, son régime juridique devrait cependant comporter les dispositions suivantes :

- La loi devrait rappeler les finalités de l'interception des communications à l'étranger, qui seraient alignées sur celles définies par l'article L. 241-3 pour les interceptions pratiquées sur le territoire. Elle ne devrait pas restreindre son champ à un mode de communication, comme le fait actuellement l'article L. 241-3, qui ne traite que des communications hertziennes. Elle devrait couvrir l'ensemble des communications électroniques, telles que définies par l'article L. 32 du code des postes et des communications électroniques[543].

- Enfin, la loi devrait prévoir que l'Autorité de contrôle des services de renseignement, appelée à se substituer à la Commission nationale de contrôle des interceptions de sécurité (CNCIS), est informée des interceptions opérées à l'étranger et peut exercer son contrôle sur leurs conditions d'exécution.

Proposition n° 39 : Définir par la loi le régime de l'interception des communications à l'étranger. La loi déterminerait les finalités de ces interceptions et habiliterait l'Autorité de contrôle des services de renseignement à exercer son contrôle sur ces activités.

Vecteur *: loi.*

L'interception des communications n'est pas le seul procédé de surveillance utilisant les techniques numériques susceptible d'être employé par les services de renseignement à des fins de prévention des atteintes à la sécurité nationale. Ceux-ci recourent également à la géolocalisation, au déchiffrement de communications cryptées et à la captation de données informatiques. Le code de procédure pénale encadre aujourd'hui manière précise le recours à de tels procédés par l'autorité judiciaire, notamment en matière de lutte contre la criminalité organisée. En revanche, comme l'a relevé une mission d'information de l'Assemblée nationale, aucun encadrement n'est prévu pour le recours à ces procédés par l'autorité administrative[544]. Or, l'exigence de prévisibilité de la loi s'applique également à la collecte de renseignements par l'autorité administrative.

La définition du régime juridique de ces « *moyens d'investigation spéciaux* », comme les qualifie la mission d'information de l'Assemblée nationale, serait donc de nature à sécuriser leur emploi par les services de renseignement. Ce régime pourrait comporter des garanties similaires à celles prévues par l'article L. 246-3 du code de la sécurité intérieure, issu de la loi de programmation militaire du

543. Selon l'article L. 32, « *on entend par communications électroniques les émissions, transmissions ou réceptions de signes, de signaux, d'écrits, d'images ou de sons, par voie électromagnétique* ».

544. J.-J. Urvoas et P. Verchère, *Rapport d'information sur l'évaluation du cadre juridique applicable aux services de renseignement*, Mission d'information de la commission des lois de l'Assemblée nationale, mai 2013.

18 décembre 2013, pour la collecte de métadonnées et la géolocalisation en temps réel : autorisation accordée par décision du Premier ministre ou des personnes spécialement désignées par lui pour une durée maximale de trente jours, pouvant être renouvelée dans les mêmes conditions de forme et de durée ; communication dans les 48 heures à l'Autorité de contrôle des services de renseignement, qui peut recommander au Premier ministre d'y mettre fin lorsqu'elle estime que le recours à ce procédé n'est pas légal.

L'encadrement du recours à ces moyens d'investigation numérique est nécessaire. Il convient cependant de veiller à ce qu'il ne se traduise pas par des contraintes excessives pour la conduite des enquêtes par les services de renseignement. Un système dans lequel chaque acte d'investigation devrait être autorisé par le Premier ministre ou un de ses subordonnés risquerait d'entraver l'action des services. Dès lors, l'autorisation donnée pourrait prévoir d'emblée, dans le respect du principe de proportionnalité, l'ensemble des moyens d'investigation numérique susceptibles d'être utilisés, au sein de la liste définie par la loi (qui comporterait la géolocalisation, le déchiffrement de communications cryptées et la captation de données informatiques).

Proposition n° 40 : Définir le régime juridique de l'utilisation par les services de renseignement, sur autorisation administrative, de certains moyens d'investigation spéciaux prenant appui sur des techniques numériques (déchiffrement, captation de données informatiques....).

Vecteur *: loi.*

Renforcer les moyens de l'AAI chargée du contrôle des opérations techniques de collecte de renseignement

La CNCIS ne dispose pas aujourd'hui de moyens suffisants pour accomplir sa mission. Compte tenu du développement considérable des communications électroniques et de l'effort important consenti par les deux dernières lois de programmation militaire pour renforcer les moyens techniques des services de renseignement, l'AAI chargée de leur contrôle devrait être dotée de moyens humains substantiels, tant sur le plan quantitatif que sur le plan qualitatif. Des compétences de haut niveau en matière d'ingénierie des communications électroniques, d'informatique et d'analyse des données apparaissent notamment requises.

Les prérogatives légales de la CNCIS n'apparaissent pas non plus suffisantes. Celle-ci ne peut contrôler que les interceptions dont elle est informée, ce qui n'apporte aucune garantie dans l'hypothèse où des interceptions seraient opérées sans être déclarées. L'AAI chargée du contrôle devrait être dotée de prérogatives de contrôle sur pièce et sur place : elle aurait le droit d'obtenir communication de tout document et de contrôler les installations et moyens techniques employés dans le cadre de la collecte de renseignements. Son champ de compétences s'étendrait aux interceptions opérées à l'étranger, comme indiqué ci-dessus, ainsi qu'à l'emploi des moyens d'investigations spéciaux. L'ensemble des membres et agents de l'AAI seraient bien sûr, comme la CNCIS aujourd'hui, astreints au respect du secret de la défense nationale.

L'extension du champ de compétences et des prérogatives justifie la reconfiguration de la CNCIS. Compte tenu des enjeux de protection des données personnelles associés à ces missions, il aurait pu être envisagé de les confier à la CNIL, avec l'avantage d'adosser le contrôle de la collecte de renseignement à une AAI déjà dotée de moyens substantiels et d'une forte légitimité en matière de protection de la vie privée. Toutefois, la forte spécificité de ces missions de contrôle, couvertes par le secret de la défense nationale, rend difficile leur conduite au sein d'une AAI généraliste comme la CNIL[545]. Il est donc préférable de maintenir une autorité spécialisée, qui pourrait être dénommée Autorité de contrôle des services de renseignement. Son collège pourrait être composé de parlementaires, de magistrats judiciaires et de membres du Conseil d'État ; le cas échéant, compte tenu de l'extension des missions, le nombre de membres du collège, aujourd'hui de trois, pourrait être relevé. Il serait également envisageable que l'Autorité ne comporte pas de parlementaire mais des membres désignés par les présidents des deux assemblées parlementaires ; en effet, la création de la DPR en 2007 permet déjà d'impliquer le Parlement dans le contrôle des services de renseignement, ce qui n'était pas le cas lorsque la CNCIS a été créée en 1991.

Proposition n° 41 : Faire de la Commission nationale de contrôle des interceptions de sécurité (CNCIS) une Autorité de contrôle des services de renseignement dotée de moyens et de prérogatives renforcés.

Vecteur : *loi.*

Même si l'AAI est dotée de prérogatives de contrôle renforcées, il lui sera difficile d'appréhender des pratiques de renseignement opérées en dehors du cadre légal et non déclarées. De telles pratiques présentent des risques particuliers pour la protection des droits fondamentaux, puisque les garanties voulues par le législateur sont écartées. Le seul moyen d'appréhender ces pratiques est bien souvent, comme l'ont montré les révélations effectuées depuis juin 2013, leur divulgation par un agent impliqué dans leur mise en œuvre.

La violation du secret de la défense nationale ne saurait devenir un droit, même lorsqu'il s'agit de dénoncer l'existence d'un programme illégal. En revanche, les agents impliqués dans la mise en œuvre des programmes de renseignement (qu'il s'agisse des agents des services de renseignement ou du personnel des opérateurs de communications impliqué dans les opérations de collecte) pourraient se voir reconnaître un droit de signalement auprès d'une Autorité de contrôle des services

545. Une enquête conduite par le G29 auprès de l'ensemble des États membres de l'Union européenne a d'ailleurs montré que seule une minorité d'États avait confié le contrôle de la collecte de renseignements par la surveillance des communications électroniques à leur autorité « *généraliste* » de protection des données. Cf. Article 29 Working Party, *Opinion 04/2014 on surveillance of electronic communications for intelligence and national security purposes*, avril 2014, 819/14/EN WP 215.

de renseignement (ACSR)[546]. Ce droit de signalement serait effectué selon des modalités sécurisées assurant la protection du secret de la défense nationale. Ils permettraient aux agents de signaler l'existence d'un programme manifestement illégal, afin que l'ACSR exerce ses prérogatives de contrôle sur la base des informations communiquées par l'agent. Aucune sanction ou mesure défavorable ne pourrait être prononcée à l'encontre d'un agent ayant exercé de bonne foi ce droit de saisine. Des dispositions de coordination avec le code pénal pourraient écarter expressément l'application des sanctions punissant les atteintes au secret de la défense nationale[547].

Proposition n° 42 : Créer un droit de signalement à l'Autorité de contrôle des services de renseignement, l'ACSR, permettant aux agents impliqués dans la mise en œuvre des programmes de renseignement de signaler des pratiques manifestement contraires au cadre légal. Ce droit de saisine serait effectué selon des modalités sécurisées assurant la protection du secret de la défense nationale.

Vecteur *: loi.*

3.5. Organiser la coopération européenne et internationale

3.5.1. Affirmer l'applicabilité du droit européen et organiser la coopération au sein de l'Union européenne

Définir un socle de règles applicables à tous les acteurs dirigeant leur activité vers la France ou l'Union européenne

Comme il a déjà été exposé (cf. 2.3.1), il conviendrait de définir un socle de règles jouant un rôle particulièrement important dans la protection des droits fondamentaux, qui seraient applicables à tous les acteurs dirigeant leur activité vers les internautes français ou européens (selon que la règle est une règle nationale ou européenne), quel que soit leur lieu d'établissement. Ce socle comprendrait les catégories de règles suivantes :

- Les règles relatives à la protection des données personnelles : la proposition de règlement prévoit qu'il sera applicable aux responsables de traitement non établis dans l'Union européenne lorsque les activités de traitement sont liées « *à l'offre de*

546. La création d'un droit de saisine analogue a été préconisée par le rapport de la commission mandatée par le président des États-Unis sur la réforme des services de renseignement : cf. *Liberty and Security in a Changing World*, décembre 2013. Le Parlement européen a appelé les États membres de l'Union européenne à explorer cette voie dans sa résolution du 12 mars 2014 sur le programme de surveillance de la NSA, les organismes de surveillance dans divers États membres et les incidences sur les droits fondamentaux des citoyens européens et sur la coopération transatlantique en matière de justice et d'affaires intérieures.

547. Articles 413-9 à 413-12 du code pénal.

biens ou de services à ces personnes concernées dans l'Union » ou « *à l'observation de leur comportement* ». Afin de faire échec à toute clause contractuelle prévoyant l'application d'une loi extra-européenne, il conviendrait de reconnaître à ce règlement le caractère d'une loi de police. S'il revient en dernier lieu au juge de décider de cette qualification, notamment au regard de la définition donnée par le règlement Rome I[548], il serait possible de la conforter en prévoyant explicitement dans le règlement que celui-ci est applicable à toute situation entrant dans son champ d'application, nonobstant toute clause contractuelle choisissant une législation extra-européenne.

- L'obligation de coopération des hébergeurs et des plateformes avec les autorités judiciaires et administratives : le II et le II *bis* de l'article 6 de la LCEN, qui prévoient les obligations de conservation des données et de coopération avec les autorités judiciaires et administratives applicables aux hébergeurs, ne définissent pas leur champ d'application territorial. La loi devrait donc prévoir que l'obligation de coopération est applicable à tout hébergeur dirigeant ses activités vers la France, la direction des activités étant appréciée selon les modalités exposées ci-dessus (1.4.2). Le même champ devrait être retenu pour les plateformes, une fois créée cette catégorie juridique.

- Le droit pénal, notamment les abus de la liberté d'expression : selon la jurisprudence de la Cour de cassation, le droit pénal français est applicable à un site destiné au public français, l'infraction étant alors regardée comme commise sur le territoire de la République (Crim., 9 septembre 2008, *Giuliano F.*, n° 07-87.281). Ceci couvre notamment l'ensemble des délits commis par voie de presse prévus par le chapitre IV de la loi du 29 juillet 1881 sur la liberté de la presse. L'état du droit est donc satisfaisant sur ce point.

Proposition n° 43 : Définir un socle de règles applicables à tous les services dirigés vers l'Union européenne ou la France (selon que la règle est européenne ou nationale), quel que soit leur lieu d'établissement. Ce socle comprendrait :

- la législation européenne relative à la protection des données personnelles, qui serait qualifiée à cette fin de « *loi de police* » au sens du droit international privé.

- l'obligation de coopération des hébergeurs et des plateformes avec les autorités administratives et judiciaires, prévue par l'article 6 de la LCEN, dont le champ d'application territorial serait explicité.

- le droit pénal, qui est déjà applicable à l'ensemble des sites destinés au public français.

Vecteur *: règlement de l'Union européenne pour la protection des données personnelles / loi pour l'obligation de coopération des hébergeurs et des plateformes.*

548. Article 9 : « *Une loi de police est une disposition impérative dont le respect est jugé crucial par un pays pour la sauvegarde de ses intérêts publics, tels que son organisation politique, sociale ou économique, au point d'en exiger l'application à toute situation entrant dans son champ d'application, quelle que soit par ailleurs la loi applicable au contrat d'après le présent règlement* ».

3.5.2. Promouvoir de nouvelles formes de coopération avec les autres espaces juridiques

Les faiblesses du *Safe Harbor* sont aujourd'hui bien connues (cf. *supra* 2.3.2). Elles tiennent notamment aux limites du modèle d'autocertification, les entreprises américaines s'engageant à respecter les principes du *Safe Harbor* mais sans que des contrôles du caractère effectif de ce respect soient assurés. La Commission européenne est aujourd'hui engagée dans une renégociation du *Safe Harbor* avec les autorités américaines. Afin d'assurer un niveau de protection satisfaisant des données personnelles des Européens, il apparaît nécessaire de ne pas se contenter d'améliorations limitées et de changer la logique même d'un système qui a échoué. Les principes du nouveau dispositif seraient les suivants :

- Le passage d'une logique d'autocertification à une logique de contrôle par un organisme tiers : les entreprises souhaitant bénéficier du *Safe Harbor* devraient se soumettre à des contrôles périodiques d'un organisme extérieur, soit la FTC, soit des certificateurs accrédités par elle. Le département du commerce américain, dont la mission première est de défendre les intérêts des entreprises américaines, ne devrait plus être impliqué dans la mise en œuvre du *Safe Harbor*[549], si ce n'est pour fournir une information générale.

- Sur le fond, la protection assurée par les principes du *Safe Harbor*, qui tiennent en trois pages, est sensiblement inférieure à celle assurée par la directive n° 95/46/CE ; l'écart serait encore accru si la proposition de règlement européen est définitivement adoptée. La Commission européenne devrait donc chercher à rehausser le niveau des engagements associés au *Safe Harbor*. Les sujets suivants pourraient notamment être traités : l'introduction des principes relatifs à la qualité des données définis par l'article 6 de la directive, qui sont aujourd'hui absents du *Safe Habor* ou ne figurent que sous une forme très atténuée ; la garantie complète du droit d'accès, sans que puisse être opposé comme aujourd'hui le caractère « *disproportionné* » de la charge de travail qu'imposerait sa mise en œuvre aux entreprises ; la création d'un droit de rectification et d'effacement ; l'obligation de notification des violations de données personnelles.

- L'association des autorités européennes aux contrôles mis en œuvre par la *Federal Trade Commission* (FTC), soit par la participation à la définition des programmes de contrôle, soit par la réalisation de contrôles conjoints.

Proposition n° 44 : Réformer le *Safe Harbor* en développant les contrôles par la *Federal Trade Commission* américaine (FTC) ou des organismes accrédités par elle, en prévoyant un droit de regard des autorités européennes sur ces contrôles et en renforçant les obligations de fond.

Vecteur *: décision de la Commission européenne.*

549. Ceci ne remet bien sûr pas en cause sa légitimité pour négocier le mécanisme du Safe Harbor avec la Commission européenne.

L'article 43 *bis* de la propositon de règlement relatif à la protection des données personnelles, introduit par le Parlement européen, dans son vote du 12 mars 2014[550], n'autorise les responsables de traitement à répondre aux demandes de divulgation de données personnelles formulées par les autorités administratives ou judiciaires d'États tiers qu'après autorisation de l'autorité de contrôle compétente. Cette disposition, qui répond à l'objectif de protéger les données personnelles des Européens face à des pratiques de collecte telles que celles mises en œuvre par le gouvernement des États-Unis, apparaît doublement excessive. D'une part, les entreprises des États concernés ne peuvent refuser de répondre aux injonctions formulées par les autorités administratives ou judiciaires de leur État, qui s'imposent à elles dans leur ordre juridique. D'autre part, il n'apparaît pas nécessaire de faire obstacle aux demandes de données formulées par les autorités administratives ou judiciaires de droit commun d'un État respectant les standards de l'État de droit ; il est en particulier peu cohérent de prévoir une telle restriction pour des États dont la Commission a reconnu le caractère adéquat du niveau de protection. Enfin, l'efficacité de ces dispositions n'est pas certaine : il est probable que les entreprises américaines seront conduites à privilégier le respect de leur ordre juridique et à ne pas informer les autorités européennes de ces transmissions de données afin de ne pas être sanctionnées.

De telles restrictions ne devraient être envisagées que comme des mesures de rétorsion à l'encontre d'un État dont les pratiques de surveillance seraient jugées excessives. La règle devrait demeurer celle prévue aujourd'hui par l'article 26 de la directive n° 1995/46/CE, selon laquelle un transfert de données peut intervenir vers un État tiers s'il est « *nécessaire ou rendu juridiquement obligatoire pour la sauvegarde d'un intérêt public important, ou pour la constatation, l'exercice ou la défense d'un droit en justice* ». Toutefois, le règlement pourrait reconnaître à la Commission le pouvoir de décider[551], au vu du caractère excessif des pratiques de surveillance d'un État tiers, de subordonner un tel transfert à l'autorisation de l'autorité de contrôle. La décision serait temporaire et devrait voir son périmètre limité au problème qui la justifie : dans le cas des États-Unis, les transferts qui posent problème sont ceux exigés par la FISC ou par les autorités administratives agissant dans le cadre de la section 702 du FISA ou par la voie des *National Security Letters*, et non ceux requis par les autorités judiciaires de droit commun. Un tel régime ne s'appliquerait pas aux États dont le niveau de protection a été reconnu adéquat.

550. Et soutenu par le G29 dans son avis précité du 10 avril 2014 sur la surveillance des communications à des fins de renseignement et de protection de la sécurité nationale.

551. Après consultation du comité représentant les États membres, prévu par l'article 87 du projet de règlement ; la procédure serait identique à celle par laquelle la Commission reconnaît le caractère adéquat du niveau de protection des données assuré par un État tiers.

Proposition n° 45 : Prévoir que les transferts de données personnelles vers certains État tiers, lorsqu'ils sont requis par les autorités administratives ou judiciaires de cet État, sont subordonnés à l'autorisation préalable de l'autorité de contrôle compétente. La décision d'appliquer ce régime à un État tiers, prise par la Commission, est temporaire et renouvelable ; elle doit être justifiée par le non-respect des standards de l'État de droit ou par le caractère excessif des pratiques de collecte de renseignement.

Vecteur *: règlement de l'Union européenne.*

Dans le cadre de la directive n° 95/46/CE comme dans celui de la proposition de règlement, la reconnaissance par la Commission du niveau adéquat de la protection des données dans un État tiers présente un caractère unilatéral. Elle permet de procéder librement à des transferts de données vers cet État tiers, mais ne comporte aucune garantie que cet État reconnaisse le système européen de protection des données et autorise le transfert de données vers l'Union européenne. Ce mode de fonctionnement n'est pas de nature à favoriser les entreprises européennes, puisqu'elles ne bénéficient pas de l'avantage reconnu aux entreprises de l'État tiers. À l'heure où un nombre croissant d'États se dotent de législations contraignantes en matière de protection des données, comme le montrent les exemples récents de la Corée du sud et du Brésil, il apparaît souhaitable de passer d'une logique de reconnaissance unilatérale à une logique de reconnaissance mutuelle. La reconnaissance resterait subordonnée à une condition objective, celle du niveau de protection adéquat dans l'État tiers ; mais elle serait soumise en outre à une réserve de réciprocité.

Ce changement de logique peut se faire à droit constant. Il suffit que la Commission européenne décide de ne reconnaître le caractère adéquat de la protection d'un État tiers qu'au vu d'engagements similaires de cet État, ou que des accords soient conclus par l'Union avec ces États tiers[552].

Proposition n° 46 : Subordonner la reconnaissance par l'UE du caractère adéquat de la protection dans des États tiers à une condition de réciprocité.

Vecteur *: action de la Commission européenne.*

En matière de lutte contre la cybercriminalité, la coopération internationale est décisive. Le degré d'implication des États dans cette lutte est inégal, plusieurs facteurs entrant en jeu : l'existence d'une législation sanctionnant les faits de cybercriminalité ; les capacités et l'efficacité des administrations et des juridictions ; la volonté de coopérer avec les autres États. Certains États sont recherchés comme

552. La procédure de conclusion d'accords est cependant plus lourde que celle de reconnaissance par la Commission du niveau de protection adéquat : en vertu de l'article 218 du traité sur le fonctionnement de l'Union européenne, les accords entre l'Union européenne et les États tiers doivent d'abord faire l'objet d'une décision du Conseil autorisant l'ouverture des négociations et donnant ses directives à la Commission, puis une nouvelle décision du Conseil après approbation du Parlement européen pour conclure l'accord négocié par la Commission.

lieu d'installation par les acteurs de la cybercriminalité en raison de leur faible implication, au point d'être parfois qualifiés de « paradis numériques » ou de « paradis cybercriminels ».

De la même manière que la lutte contre le blanchiment ou contre les paradis fiscaux avait été mise en place grâce à la création du Groupe d'action financière (GAFI), organisme intergouvernemental créé par le G7 en 1989, un groupe d'action d'action interétatique pourrait être créé pour lutter contre la cybercriminalité tolérée par des États non coopératifs. Le Conseil de l'Europe, au sein duquel a été signée la convention de Budapest, apparaît comme l'organisation la mieux placée pour établir une telle liste, selon une méthodologie qui serait définie avec les États parties à la convention.

Proposition n° 47 : Créer un groupe d'action interétatique, sur le modèle du Groupe d'action financière (GAFI), pour définir des recommandations en matière de lutte contre la cybercriminalité et publier une liste d'États non coopératifs.

Vecteur *: action du Conseil de l'Europe.*

3.5.3. Rééquilibrer la gouvernance d'internet

Le rééquilibrage de la gouvernance d'Internet implique à court terme une réforme des institutions existantes ; à plus long terme, il conviendrait de promouvoir la conclusion d'une convention internationale relative aux libertés fondamentales et aux principes de la gouvernance d'internet.

La réforme des institutions existantes

En dépit des critiques dont il est la cible (cf. 2.3.3), le modèle « multiacteurs », dont la caractéristique principale est d'associer l'ensemble des parties prenantes (États, société civile, entreprises) à la prise de décision, a fait la preuve de son efficacité en permettant un développement extrêmement rapide du réseau internet. De ce point de vue, abandonner ce modèle au profit d'un modèle intergouvernemental, n'apparaît pas souhaitable, dès lors que ce dernier risquerait de s'avérer incapable d'intégrer les innovations technologiques majeures à venir. Pour autant, il apparaît nécessaire de réformer le modèle « multiacteurs » tel qu'il fonctionne aujourd'hui afin de le rendre plus démocratique et plus représentatif du caractère proprement mondial du réseau Internet.

La réforme des instances de gouvernance de l'Internet concerne en premier lieu l'ICANN. Une situation dans laquelle l'ICANN, parce qu'elle ne rendrait plus de comptes au gouvernement des États-Unis, ne rendrait plus de comptes qu'à elle-même, serait sans doute pire que la situation antérieure. L'étude du Conseil d'État de 1998 sur internet *et les réseaux numériques* avait souligné que l'organisme chargé de la régulation du système des noms de domaine était investi d'une mission d'intérêt général[553] et devait être guidé par un « *mandat* » international.

553. Dans le même sens, le Conseil d'État statuant au contentieux a d'ailleurs jugé que l'organisme en charge de la gestion du .fr, l'AFNIC, était investi d'une mission de service public

Le processus de réforme en cours doit être l'occasion de donner une traduction concrète à ces exigences. Deux orientations doivent donc être suivies : l'une a trait à une plus grande responsabilisation des instances dirigeantes de cette organisation ; l'autre à une meilleure prise en compte des intérêts défendus par les États, qui sont les dépositaires de l'intérêt général.

L'appel en faveur d'une plus grande responsabilisation des instances dirigeantes de l'ICANN a été formulé par un grand nombre d'États et d'organisations issus de la société civile, en dernier lieu lors du forum *Netmundial* organisé au Brésil en avril 2014. À l'issue de ce forum a en effet été adoptée une déclaration de principes au sein de laquelle figure une définition du principe d'*accountability* susceptible de structurer la gouvernance d'Internet à l'avenir. Cette définition repose sur la mise en place de mécanismes indépendants susceptibles de constituer des contre-pouvoirs et sur la création de voies de recours contre les décisions prises. Or ce sont de tels contre-pouvoirs et de tels recours qui font aujourd'hui défaut à l'ICANN, dont les décisions sont prises par son conseil d'administration, sans que leur bien-fondé puisse être contesté devant aucune instance. En effet, les mécanismes de révision existants ne donnent lieu qu'à des recommandations dépourvues de portée contraignante, dont le conseil d'administration doit seulement « *prendre connaissance* ». Il est donc nécessaire d'instaurer, au sein de l'ICANN des contre-pouvoirs permettant de contester les décisions prises par le conseil d'administration, voire de mettre en cause sa responsabilité. Cet objectif pourrait être atteint si l'on dotait d'une portée contraignante les mécanismes de révision existants et si l'on instaurait une assemblée générale au sein de laquelle seraient représentées l'ensemble des parties prenantes, et devant laquelle le conseil d'administration serait responsable.

L'appel en faveur d'une meilleure prise en compte des intérêts défendus par les États est quant à lui fondé sur l'idée que les États ne sauraient être considérés comme des « parties prenantes » comme les autres, dès lors qu'ils ont vocation à être garants de l'intérêt général. Dans ces conditions, il pourrait être opportun de promouvoir des mécanismes par lesquels le comité représentant les gouvernements (GAC), qui n'a aujourd'hui qu'un rôle consultatif, serait susceptible de s'opposer à une décision prise par le conseil d'administration. Une telle évolution supposerait néanmoins de faire évoluer la composition du GAC, où une majorité d'États est représentée à un niveau plus technique que politique.

Proposition n° 48 : Promouvoir la démocratisation de l'ICANN, en :

- créant une assemblée générale rassemblant l'ensemble des parties prenantes et pouvant mettre en cause la responsabilité du conseil d'administration ;

- renforçant les mécanismes de recours internes, par exemple en dotant d'une portée contraignante le mécanisme d'*Independent Review Panel* ;

- permettant au comité représentant les gouvernements (GAC) d'adopter des résolutions contraignantes.

Vecteur *: modification des statuts de l'ICANN.*

(CE 10 juin 2013, *M. A.*, n° 327375, à mentionner aux tables).

L'internationalisation des institutions existantes constitue le second axe de réforme en matière de gouvernance d'internet. Né aux États-Unis, le réseau internet demeure dominé par cet État dans sa conception, son fonctionnement et son évolution, alors même que son centre de gravité s'est déplacé vers l'Europe et les pays émergents.

Outre les évolutions institutionnelles en cours concernant l'ICANN, une diversification des profils des dirigeants siégeant au sein des instances de gouvernance d'internet (l'ICANN mais aussi l'IETF, le W3C et l'*Internet Society*) est nécessaire. Elle serait favorisée par des critères de sélection plus stricts afin de s'assurer que sont effectivement représentés les différents continents et les grandes aires linguistiques (notamment la francophonie). Du point de vue de la France et de l'Union européenne, la pleine inscription dans ce processus appelle, la définition d'une stratégie d'influence structurée passant, notamment, par la constitution d'un vivier de cadres européens susceptibles d'occuper des postes de responsabilité au sein de ces organisations.

Proposition n° 49 : Diversifier la composition des instances de gouvernance d'internet, par des critères de sélection imposant une réelle diversité linguistique et géographique et la mise en place de stratégies d'influence au niveau de la France et de l'Union européenne.

Vecteur *: modification des statuts de ces instances, action du Gouvernement français et de l'Union européenne.*

Promouvoir l'adoption d'une convention internationale relative aux libertés fondamentales et aux principes de la gouvernance d'internet

La gouvernance d'internet a toujours reposé jusqu'ici sur le droit souple. Ce modèle, qui a porté le développement d'internet, rencontre cependant certaines limites. Souvent présenté comme une manière de limiter le rôle des gouvernements, il ne crée en réalité aucune obligation pour les États de respecter les libertés fondamentales. Une convention internationale qui énoncerait les grands principes devant être respectés par les États serait plus protectrice des libertés. En ne stipulant rien sur les modalités de la gouvernance, elle ne porterait pas atteinte à l'efficacité de celle-ci.

Plusieurs évolutions récentes témoignent d'une maturation des esprits qui pourrait préparer l'adoption d'une telle convention. Le concepteur du *web*, Tim Berners-Lee, pourtant président d'une des principales instances productrices de droit souple (le *World Wide Web Consortium*), a appelé à l'adoption d'une « *Magna Carta* » d'internet : il estime qu'un tel instrument est aujourd'hui nécessaire pour protéger le caractère neutre et ouvert d'internet, ainsi que le droit à la vie privée et la liberté d'expression. Plusieurs instruments de droit souple ont, au cours des dernières années, énoncé les grands principes qui pourraient être repris dans une

convention internationale. Une telle évolution du droit souple vers le droit dur a été observée à de multiples reprises en droit international, notamment en matière de droits de l'homme[554].

Une convention internationale relative aux libertés fondamentales et aux principes de la gouvernance d'internet devrait notamment énoncer les principes suivants :

- la liberté d'expression ;
- le droit à la vie privée et à la protection des données personnelles ;
- le caractère neutre et ouvert de l'architecture d'internet ;
- l'interdiction de porter atteinte à la sécurité du réseau ;
- l'obligation de coopérer dans la lutte contre la cybercriminalité ;
- le caractère multiacteurs et la transparence de la gouvernance d'internet.

Proposition n° 50 : Promouvoir l'adoption d'une convention internationale relative aux libertés fondamentales et aux principes de la gouvernance d'internet.

Vecteur *: convention internationale.*

554. La Déclaration universelle des droits de l'homme de 1948 a ainsi inspiré les deux pactes des Nations unies de 1966. Les conventions des Nations unies relatives aux droits de l'enfant et aux droits des personnes handicapées ont de même été précédées par des résolutions non contraignantes.

Conclusion

En choisissant ce sujet, le Conseil d'État en connaissait la complexité et les difficultés. Au terme de cette étude, il convient de confronter les objectifs qu'elle s'était assignés aux orientations qu'elle retient et aux propositions qu'elle émet.

Deux écueils devaient, tout d'abord, être évités. Le Conseil d'État s'est tout d'abord gardé d'une approche « idéologique » d'un sujet qui y est pourtant propice, en tenant également à distance les postures libertaire et sécuritaire trop souvent adoptées pour traiter du domaine des technologies de l'internet. Il n'a pas davantage retenu une démarche exclusivement académique portant sur l'analyse des enjeux juridiques du numérique. Conseiller du Gouvernement, il a plutôt souhaité procéder de manière pragmatique, en observant tous les usages ou pratiques des technologies numériques pour en dégager un *corpus* d'une cinquantaine de propositions visant à y renforcer l'exercice des droits fondamentaux, sans pour autant altérer le potentiel d'innovation de ces technologies.

Quatre grandes hypothèses de travail ont été validées par l'étude.

- La première postulait que **le numérique représente une mutation radicale qui affecte et modifie le contenu des droits fondamentaux.** Le Conseil d'État a pu légitimement soutenir en 1998 [555] « *qu'il n'existe pas et qu'il n'y a nul besoin, d'un droit spécifique de l'internet et de réseaux : ceux-ci sont des espaces dans lesquels tout type d'activité peut être pratiqué et toutes les règles régissant un domaine particulier (publicité, fiscalité, propriété intellectuelle…) ont vocation à s'appliquer* ». Cette affirmation doit être aujourd'hui fortement nuancée. Face à l'explosion numérique, le droit s'est déjà beaucoup transformé et il est encore à la recherche d'un point d'équilibre. L'étude montre le décalage entre le rythme des innovations dont le numérique est porteur (réseaux sociaux, internet mobile, audiovisuel sur internet, géolocalisation, reconnaissance faciale, données massives – *Big Data* –, objets connectés, intelligence artificielle) et le temps d'adaptation du régime juridique des droits fondamentaux. Il est néanmoins possible de rendre applicables au numérique des concepts juridiques antérieurs à son apparition, en adaptant les instruments dont dispose la puissance publique pour les mettre en œuvre. On rappellera ici, sans être exhaustif, certaines propositions concrètes de l'étude qui traduisent des évolutions significatives : le droit et les devoirs pour les individus, de protéger leurs données personnelles (autodétermination informationnelle) ; la définition d'une catégorie juridique des plateformes accompagnées des obligations

555. *Internet et les réseaux numériques*, collection, les études du Conseil d'État, 1998, La documentation Française, 2000, p.14

qui s'attachent au principe de loyauté dont ces dernières doivent faire preuve ; la mise en œuvre du droit au déréférencement sur les moteurs de recherche et l'élaboration des modalités juridiques d'une décision unique de déréférencement ; la définition d'un droit des algorithmes prédictifs ; une proposition de réforme du régime de la concentration en matière de presse d'information pour tenir compte de nouveaux modes de support de communication ; une nouvelle réponse à la nécessaire conciliation entre la protection de la vie privée et la conservation des métadonnées à des fins de prévention des atteintes à la sécurité nationale.

- La deuxième hypothèse proposait de faire de la réponse à **l'ambivalence intrinsèque** qui caractérise le phénomène numérique, un critère de la pertinence des propositions. L'étude montre, à maintes reprises, qu'une intervention trop vigoureuse destinée à corriger les aspects négatifs du numérique risque, dans le même mouvement, d'en entraver le potentiel positif. La difficulté d'apporter des réponses équilibrées tient à ce que le numérique ouvre de nouveaux espaces de libertés, en même temps qu'il recèle des risques et des menaces. Comme d'autres technologies, le numérique peut avoir des usages bénéfiques ou néfastes, mais parce qu'il « fait système », il n'est pas un outil docile aux mains de son maître, il porte en lui-même des conséquences qui échappent à la volonté de ses utilisateurs. Ce caractère « Janus » et « biface » du numérique a impliqué le choix de **mesures adaptées et proportionnées**.

- La troisième hypothèse soutenait qu'en matière de régulation d'internet et d'usage des technologies numériques, **le droit souple est parfois mieux à même de fournir des solutions juridiques praticables,** parce qu'acceptées par les acteurs privés comme publics. Parmi les propositions que l'étude présente, plus d'une dizaine mettent en avant le recours aux recommandations, aux guides de bonnes pratiques, à l'homologation des codes de conduite professionnels, à la certification ou à la médiation. Il est en outre proposé de renforcer le rôle de conseil et de référent des autorités administratives indépendantes comme la CNIL, le CSA, ou l'ARCEP.

- La quatrième hypothèse retenait que les **internautes européens doivent se voir appliquer en priorité des règles européennes** sans que la recherche de nouveaux modes de coopération avec les autres espaces juridiques soit pour autant négligée. L'étude propose la modification ou le renforcement, en ce sens, d'un socle de règles de l'Union choisies en raison de leur importance particulière dans la protection des droits fondamentaux ou de l'ordre public et qui doivent s'appliquer aux responsables de traitements établis hors de l'Union européenne.

Les 50 propositions de l'étude résultent de **la validation de ces quatre hypothèses**. Elles s'inscrivent nécessairement dans le cadre juridique européen.

La « centralité » de l'Europe dans le domaine des technologies de communication se manifeste, à la façon d'une « ombre portée », sur les propositions de l'étude de trois manières différentes.

En premier lieu, les propositions ont l'ambition de **respecter la meilleure articulation entre le droit européen et le droit interne**. En effet, nombre des mesures de l'étude relèvent de la compétence des institutions de l'Union européenne, soit parce qu'elles impliquent une modification du droit de l'Union existant, soit parce que l'Union européenne constitue, en opportunité, le niveau pertinent d'action. Ainsi, la proposition de règlement européen relatif à la protection des données personnelles, dont la procédure d'adoption est en cours, est le réceptacle naturel de plusieurs propositions importantes de l'étude. Les autorités françaises chargées des négociations sur ce texte pourront y trouver des éléments de réflexion et, peut-être, des arguments de négociation. D'autres propositions relèvent du G29 qui regroupe les différentes autorités de protection de données de l'Union. Ainsi en est-il de la proposition relative à la mise œuvre du droit de déréférencement sur les moteurs de recherche ou de celle sur la promotion des technologies de renforcement de la vie privée. D'autres enfin sont de la compétence de la Commission européenne.

Toutefois, il est apparu au Conseil d'État qu'un nombre, certes limité, de **propositions pouvaient être portées en priorité par les autorités nationales**. Les délais de mise au point des directives ou règlements peuvent être longs et impliquer, par conséquent, des initiatives des autorités françaises en matière, par exemple, de protection des données personnelles, de garanties en faveur des organes de presse ou encore de réglementation de la responsabilité des plateformes numériques. D'autres sujets touchent aux **intérêts fondamentaux de notre pays** : il en est ainsi des modalités de conservation des données de communication à des fins de prévention ou de répression, qui doivent apporter les garanties nécessaires à la protection des droits et libertés tout en préservant l'efficacité de notre système de sécurité. La position française sur le juste équilibre entre ces deux objectifs doit être défendue au niveau européen.

En deuxième lieu, les propositions de l'étude qui visent à **développer le potentiel d'innovation du numérique** doivent apporter des réponses permettant à l'Europe de relever les défis économiques liés à ces technologies et de faire contrepoids aux autres puissances mondiales impliquées dans ce processus. L'industrie de l'internet est aujourd'hui massivement américaine et, à un moindre degré, asiatique ; l'Europe a été distancée sur la génération actuelle des plateformes. L'innovation, la liberté d'entreprendre peuvent favoriser l'apparition, en Europe, de nouvelles formes d'organisation et de création de valeur numérique, notamment grâce aux objets connectés. **L'enjeu n'est pas qu'économique**. Le droit doit intervenir pour favoriser une autre vision du numérique, qui prendrait plus largement en compte les enjeux de **la connaissance, de l'éducation et de la culture**. Il s'agit de faire contrepoids aux pratiques dominantes d'internet aujourd'hui marquées par le recours massif aux instruments de traçage et à un modèle économique moins ouvert et plus concentré qu'il ne fut à son origine. Là réside aussi l'ambition des propositions du Conseil d'État ; le droit, loin d'être un obstacle, serait un atout en maitère de sécurité juridique et de développement économique.

En troisième lieu, **l'Europe doit affirmer ses valeurs**. Elle doit éviter de fixer des règles qui s'imposent davantage à ses propres acteurs économiques qu'à ceux dont le pays d'origine est extérieur à l'Union européenne et qui risquent de désavantager ses propres citoyens et ses propres entreprises. C'est l'enjeu de la territorialité de la norme. L'Europe ne doit pas être non plus naïve, ni sous-estimer son influence : un espace de 500 millions d'habitants à revenu élevé, et de plus de 400 millions d'internautes à haut niveau d'instruction est en capacité de faire valoir **l'influence de ses standards,** qu'ils soient **juridiques, techniques, économiques, sociaux et, bien sûr, culturels**.

***

Lorsqu'il s'est engagé dans cette étude, le Conseil d'État savait qu'il était attendu sur le terrain de la défense des droits fondamentaux. Il savait aussi qu'il ne devait pas se borner à la seule position – au demeurant fort légitime – de gardien des droits des personnes et, ainsi, prendre le risque de restreindre les effets dynamiques des technologies numériques. Il a souhaité prendre en considération toutes les potentialités du numérique, tout particulièrement celles qui en font le vecteur d'une économie qui favorise la croissance et l'emploi.

Le Conseil d'État aurait manqué à son office et son étude annuelle, à son objectif, si n'avaient pas été concomitamment traités les deux aspects d'une même réalité : l'innovation numérique et le respect des droits fondamentaux des citoyens. Ce fut son ambition que de tenir cette ligne de crête.

Récapitulatif des mesures proposées

Définir les principes fondant la protection des droits fondamentaux à l'ère du numérique (3.1.)

Le droit sur les données personnelles : un droit à l'autodétermination plutôt qu'un droit de propriété (3.1.1.)

Proposition n° 1

Concevoir le droit à la protection des données personnelles comme un droit à « *l'autodétermination informationnelle* », c'est-à-dire le droit de l'individu de décider de la communication et de l'utilisation de ses données à caractère personnel.

Inscrire cette conception dans la proposition de règlement relatif à la protection des données à caractère personnel ou, dans l'attente du règlement, dans la loi du 6 janvier 1978.

Ne pas faire entrer les données personnelles dans le champ du droit de propriété patrimonial des personnes.

Vecteur : règlement de l'Union européenne ou loi.

Neutralité des réseaux, loyauté des plateformes (3.1.2.)

Proposition n° 2

Consacrer le principe de neutralité des opérateurs de communications électroniques dans les termes votés par le Parlement européen le 3 avril 2014, sous trois réserves :

- Revenir à la définition des mesures de gestion de trafic de la proposition de la Commission ;

- Revenir à la définition plus large des « services spécialisés », mais avec des contreparties : information préalable de l'autorité de régulation concernée sur le projet de convention ; droit d'opposition si risque manifeste de dégradation de la qualité de l'internet en-deçà d'un niveau satisfaisant ; droit de suspension de l'autorité de régulation s'il s'avère que qualité de l'internet est dégradée ;

- Droit des opérateurs d'exiger un paiement des fournisseurs de contenus, dans le cadre d'une facturation asymétrique, lorsqu'ils représentent à eux seuls une part significative du trafic.

Vecteur : loi ou règlement de l'Union européenne.

Proposition n° 3

Définir la catégorie juridique des plateformes, distincte de celle des simples hébergeurs passifs. Seraient qualifiés de plateformes les services de référencement ou de classement de contenus, biens ou services édités ou fournis par des tiers et partagés sur le site de la plateforme. Les plateformes seraient soumises à un principe de loyauté.

Vecteur : directive de l'Union européenne.

Renforcer les pouvoirs des individus et de leurs groupements (3.2.)

Renforcer les capacités d'action individuelle (3.2.1.)

Proposition n° 4

Donner à la CNIL et à l'ensemble des autorités de protection des données européennes une mission explicite de promotion des technologies renforçant la maîtrise des personnes sur l'utilisation de leurs données.

Envisager notamment les actions suivantes :

- Lancer au niveau européen une concertation multiacteurs dans le but de susciter l'émergence des solutions technologiques les plus prometteuses en termes de renforcement de la vie privée ;

- Promouvoir la diffusion gratuite d'outils de renforcement de la vie privée par les FAI, soit dans un cadre volontaire, soit en l'imposant par la loi comme c'est le cas pour les logiciels de contrôle parental ;

- Dans le cadre de la standardisation des politiques d'utilisation des données personnelles prévue par le projet de règlement européen, susciter le développement de règlements-types définissant des polices d'utilisation, auxquels un grand nombre d'internautes adhéreraient et que les entreprises seraient donc conduites à prendre en compte pour définir leur propre politique.

- Développer l'intervention de prestataires « *tiers de confiance* », afin de garantir que seules les données dont la personne a autorisé la divulgation sont diffusées.

Vecteur : Loi, règlement de l'Union européenne, action de la CNIL et des autres autorités européennes de protection des données.

Proposition n° 5

Mettre en œuvre de manière efficace le droit au déréférencement consacré par l'arrêt *Google Spain*, en :

- Donnant aux éditeurs des sites dont le déréférencement est demandé la possibilité de faire valoir leurs observations ;

- Explicitant par des lignes directrices la doctrine de mise en œuvre de *Google Spain* par les autorités de protection des données ;

- Organisant les conditions d'une décision unique de déréférencement, soit par accords de reconnaissance mutuelle des décisions de déréférencement prises par les exploitants de moteurs de recherche, soit par un dispositif légal d'extension à tous les exploitants d'une décision prise par l'un d'entre eux, sous réserve de son homologation par un juge.

Vecteur : lignes directrices du G29 pour les deux premiers points ; accord entre les exploitants de moteurs de recherche ou loi pour le troisième.

Proposition n° 6

Définir les obligations des plateformes envers leurs utilisateurs, découlant du principe de loyauté :

- pertinence des critères de classement et de référencement mis en œuvre par la plateforme au regard de l'objectif de meilleur service rendu à l'utilisateur ;

- information sur les critères de classement et de référencement ;

- définition des critères de retrait de contenus licites en termes clairs, accessibles à tous, et non discriminatoires ;

- mettre l'utilisateur ayant mis en ligne un contenu en mesure de faire valoir ses observations en cas de retrait de celui-ci ;

- en ce qui concerne les utilisateurs commerciaux, notification préalable, avec un délai de réponse raisonnable, des changements de la politique de contenus ou de l'algorithme susceptibles d'affecter le référencement ou le classement.

Vecteur : directive de l'Union européenne ou droit souple (chartes d'engagements des plateformes)

Proposition n° 7

Mettre en œuvre le droit d'alerte pour les salariés des organismes traitant des données personnelles, par des processus d'information et de déclaration placés sous la responsabilité de la CNIL.

Vecteur : action de la CNIL.

Renforcer les capacités d'action collective (3.2.2.)

Proposition n° 8

Créer une action collective, distincte de l'action de groupe, destinée à faire cesser les violations de la législation sur les données personnelles. Cette action serait exercée devant le tribunal de grande instance par les associations agréées de protection de consommateurs ou de défense de la vie privée et des données personnelles.

Vecteur : loi.

Proposition n° 9

Mettre en *Open Data* toutes les déclarations et autorisations de traitements de données.

Vecteur : action de la CNIL.

Dans le cadre du projet de règlement européen, prévoir la publication sur le site de l'autorité de protection des données par les délégués à la protection des données, d'un rapport d'information annuel sur les traitements mis en œuvre par leur organisme.

Vecteur : règlement de l'Union européenne.

Proposition n° 10

Développer la participation des utilisateurs des plateformes à l'élaboration des règles définissant les contenus pouvant être mis en ligne sur leur site.

Vecteur : droit souple (charte d'engagements des plateformes) ; recommandations de l'autorité de régulation compétente.

Proposition n°11

Confier à la CNIL ou au Conseil national du numérique une mission permanente d'animation de la délibération collective sur les enjeux éthiques liés au numérique.

Vecteur : loi pour la CNIL, décret pour le CNNum.

Redéfinir les instruments de la protection des droits fondamentaux et repenser le rôle des autorités publiques (3.3.)

Tirer les conséquences du passage à l'ère de l'économie des données personnelles (3.3.1.)

Proposition n° 12

Afin de sécuriser le développement du *Big Data* en Europe, maintenir sans ambiguïté dans la proposition de règlement européen la liberté de réutilisation statistique des données personnelles, quelle que soit la finalité initiale de leur traitement, en prévoyant pour seule condition que cette réutilisation soit entourée de garanties d'anonymat appropriées.

Vecteur : le règlement de l'Union européenne

Proposition n° 13

Renforcer le rôle de conseil et d'accompagnement des responsables de traitement par la CNIL.

Vecteur : action de la CNIL.

Proposition n° 14

Créer un *certificat de conformité (rescrit « données personnelles »*).

Vecteur : loi.

Proposition n° 15

Clarifier le champ des traitements soumis en raison de leurs risques à des obligations particulières telles que la réalisation d'une étude d'impact ou la consultation préalable de l'autorité de contrôle, en définissant dans le règlement la liste des catégories de traitement concernées. La soumission à l'obligation de consultation préalable ne doit pas dépendre du résultat de l'étude d'impact.

Vecteur : règlement de l'Union européenne.

Proposition n° 16

Créer une procédure d'homologation des codes de conduite professionnels élaborés au niveau national ou européen.

Vecteur : règlement de l'Union européenne.

Proposition n° 17

Développer la normalisation en matière de sécurité des traitements de données personnelles.

Vecteur : règlement de l'Union européenne.

Proposition n° 18

Participer et organiser la transition vers le nouveau cadre juridique issu du règlement, par une coopération entre le gouvernement, la CNIL et les principaux acteurs professionnels concernés.

Vecteur : action du gouvernement, de la CNIL et des principaux acteurs professionnels concernés.

Proposition n° 19

Créer pour les catégories de traitements présentant les risques les plus importants une obligation de certification périodique (complétant l'examen *a priori* par l'autorité de contrôle dans le cadre de la procédure de consultation préalable) par un organisme tiers indépendant et accrédité par l'autorité de contrôle.

Vecteur : règlement de l'Union européenne.

Proposition n° 20

Porter une attention particulière aux transmissions de données personnelles d'une entité à une autre en :

- codifiant dans la loi la jurisprudence relative à la nullité des transactions portant sur des fichiers non déclarés ou non autorisés à la CNIL (*vecteur : loi*) ;

- incitant les acteurs procédant de manière récurrente à de telles transactions à en tenir un registre (*vecteur : code de conduite professionnel*) ;

- incitant à fournir aux personnes exerçant leur droit d'accès une liste complète des entités auxquelles leurs données ont été communiquées (*vecteur : code de conduite professionnel*).

Proposition n° 21

Mettre à l'étude la création d'un numéro national unique d'identification non signifiant.

Vecteur : action du Gouvernement et de la CNIL.

Proposition n° 22

Permettre le recours au NIR pour les traitements de données personnelles ayant pour fin la recherche dans le domaine de la santé et autorisés par la CNIL en vertu du chapitre IX de la loi du 6 janvier 1978. Admettre l'utilisation du NIR comme identifiant national pour les données de santé.

Vecteur : loi ; action de la CNIL.

Définir un droit des algorithmes prédictifs (3.3.2.)

Proposition n° 23

Pour assurer l'effectivité de l'interdiction de fonder une décision sur la seule mise en œuvre d'un traitement automatisé, confirmer que l'intervention humaine dans la décision doit être réelle et pas seulement formelle. Indiquer dans un instrument de droit souple les critères d'appréciation du caractère effectif de l'intervention humaine.

Vecteur : règlement de l'Union européenne et droit souple (recommandation de la CNIL ou avis du G29).

Proposition n° 24

Imposer aux auteurs de décisions s'appuyant sur la mise en œuvre d'algorithmes une obligation de transparence sur les données personnelles utilisées par l'algorithme et le raisonnement général suivi par celui-ci. Donner à la personne faisant l'objet de la décision la possibilité de faire valoir ses observations.

Vecteur : loi ou règlement de l'Union européenne.

Proposition n° 25

Dans le cadre de l'article 44 de la loi du 6 janvier 1978, et dans le respect du secret industriel, développer le contrôle des algorithmes par l'observation de leurs résultats, notamment pour détecter des discriminations illicites, en renforçant à cette fin les moyens humains dont dispose la CNIL.

Vecteur : action de la CNIL.

Proposition n° 26

Analyser les pratiques de différenciation des prix reposant sur l'utilisation des données personnelles, mesurer leur développement et déterminer celles qui devraient être qualifiées de pratiques commerciales illicites ou déloyales, et sanctionnées comme telles.

Vecteur : action de la DGCCRF ; saisine du Conseil national de la consommation de l'Autorité de la concurrence ; loi à l'issue de la réflexion.

Proposition n° 27

Encourager la prise en compte de la diversité culturelle dans les algorithmes de recommandation utilisés par les sites internet diffusant des contenus audiovisuels ou musicaux.

Vecteur : droit souple ou conventions conclues avec le CSA.

Organiser la répartition des rôles entre acteurs publics et acteurs privés dans la lutte contre les contenus illicites (3.3.3.)

Proposition n° 28

Aligner le régime de responsabilité civile et pénale des plateformes sur celui des hébergeurs. Prévoir une obligation pour les hébergeurs et les plateformes d'empêcher, durant un délai déterminé, la réapparition des contenus ayant fait précédemment l'objet de retrait. Cette obligation serait prononcée par l'autorité administrative.

Vecteur : loi (pour les plateformes, après l'intervention de la directive de l'Union européenne créant la catégorie juridique des plateformes).

Proposition n° 29

Encadrer l'utilisation des outils de surveillance automatique des contenus mis en œuvre volontairement par les plateformes en prévoyant une obligation de transparence sur l'utilisation de ces outils, leur fonctionnement et l'étendue des blocages de contenus qu'ils entraînent.

Vecteur : loi (après l'intervention de la directive de l'Union européenne créant la catégorie juridique des plateformes).

Adapter les instruments de la promotion du pluralisme des médias (3.3.4.)

Proposition n° 30

Revoir le contrôle de la concentration dans les médias, et notamment les quotas de diffusion et la mesure des bassins d'audience utilisés pour la limiter, afin de mieux garantir le pluralisme au regard de l'ensemble des modes de diffusion contemporains.

Vecteur : concertation en vue d'une loi.

Développer la médiation pour régler les litiges liés à l'utilisation des technologies numériques (3.3.5.)

Proposition n° 31

Mettre en place un système de médiation facilement accessible pour régler les petits litiges entre personnes privées liés à l'utilisation des technologies numériques, tels que ceux concernant les données personnelles, les atteintes à la réputation sur internet ou le retrait de contenus mis en ligne.

Vecteur : accord entre les parties prenantes ou loi.

Assurer le respect des droits fondamentaux dans l'utilisation du numérique par les personnes publiques (3.4.)

Poursuivre l'ouverture des données publiques tout en prévenant les risques pour la vie privée (3.4.1.)

Proposition n° 32

Afin de promouvoir le développement de l'*open data* auprès des personnes publiques, notamment les collectivités territoriales :

- Adopter une charte d'engagements et de bonnes pratiques signée par l'État, les associations de collectivités territoriales et les représentants des utilisateurs des données publiques, et promouvoir l'adhésion des personnes publiques à cette charte.

- Accroître le rôle d'appui des services de l'État aux collectivités territoriales souhaitant ouvrir leurs données publiques

Vecteur : droit souple (charte d'engagements et de bonnes pratiques) et décret.

Proposition n° 33

Pour les données publiques comportant des données personnelles, maîtriser les conditions de leur ouverture afin de limiter étroitement le risque de réidentification.

À cette fin :

- Faire définir par la CNIL, en concertation étroite avec le comité du secret statistique et la CADA, des standards d'anonymisation ;

- Constituer au sein de chaque ministère un pôle d'expertise en matière d'anonymisation, *a priori* au sein du service statistique ministériel ;

- Assurer l'accessibilité de ces services d'expertise aux collectivités territoriales qui en font la demande auprès du préfet.

- Lorsque le risque de réidentification ne peut être écarté, définir une procédure d'accès sur autorisation plutôt que de mettre en ligne, en particulier lorsque sont en cause des données sensibles (par exemple des données de santé, des données fiscales ou des informations sur les difficultés sociales des personnes).

Vecteur : Droit souple (recommandations de bonnes pratiques) et organisation des services de l'État. Le cas échéant, dispositions législatives pour définir les procédures d'accès sur autorisation.

Renforcer les garanties entourant l'usage des fichiers de police (3.4.2.)

Proposition n° 34

Préciser, en s'inspirant des dispositions relatives au fichier « *Traitements d'antécédents judiciaires* » (TAJ), les conséquences à tirer des décisions judiciaires (classement sans suite, non-lieu, relaxe et acquittement) quant à l'effacement des données relatives aux personnes mises en cause, pour le fichier automatisé des empreintes digitales (FAED) et le fichier national automatisé des empreintes génétiques (FNAEG).

Vecteur : décret pour le FAED, loi pour le FNAEG.

Proposition n° 35

Définir un plan d'apurement des erreurs et insuffisances du fichier « *Traitements d'antécédents judiciaires* » (TAJ), notamment sur les suites judiciaires données aux mises en cause, afin de mettre à jour l'ensemble des fiches qui y sont contenues.

Vecteur : action du ministère de la justice et du ministère de l'intérieur.

Proposition n° 36

Mettre en œuvre la décision n° 2010-25 QPC du 16 septembre 2010 du Conseil constitutionnel, en modulant la durée de conservation des données dans le fichier national automatisé des empreintes génétiques (FNAEG) en fonction de la gravité de l'infraction et de la minorité de la personne au moment de l'enregistrement.

Vecteur : décret en Conseil d'État.

Proposition n° 37

Définir un régime d'autorisation aux formalités allégées (spécifications du traitement moins précises et autorisation délivrée par la CNIL dans le cadre de l'article 25 de la loi du 6 janvier 1978) pour les expérimentations de traitements de données régis par les articles 26 et 27 de la loi du 6 janvier 1978.

Vecteur : loi.

Conjuguer le plein respect des droits fondamentaux et l'efficacité de la surveillance des communications électroniques à des fins de renseignement (3.4.3.)

Proposition n° 38

Tirer les conséquences de l'arrêt *Digital Rights Ireland* en ce qui concerne l'accès aux métadonnées, en :

- réservant l'accès à des fins de police judiciaire aux crimes et aux délits d'une gravité suffisante ;

- réexaminant les régimes prévoyant l'accès de certaines autorités administratives pour des finalités autres que la sécurité intérieure (par exemple HADOPI, ANSSI, administration fiscale, AMF), et notamment les circonstances dans lesquelles cet accès peut être demandé et les données peuvent être communiquées ;

- modulant la période accessible en fonction de la finalité et de la gravité des infractions ;

- étendant, pour l'accès aux métadonnées, les règles spécifiques de protection qui bénéficient aux parlementaires, aux avocats, aux magistrats et aux journalistes.

Vecteur : loi.

Proposition n° 39

Définir par la loi le régime de l'interception des communications à l'étranger. La loi déterminerait les finalités de ces interceptions et habiliterait l'Autorité de contrôle des services de renseignement à exercer son contrôle sur ces activités.

Vecteur : loi.

Proposition n° 40

Définir le régime juridique de l'utilisation par les services de renseignement, sur autorisation administrative, de certains moyens d'investigation spéciaux prenant appui sur des techniques numériques (déchiffrement, captation de données informatiques...).

Vecteur : loi.

Proposition n° 41

Faire de la Commission nationale de contrôle des interceptions de sécurité (CNCIS) une Autorité de contrôle des services de renseignement dotée de moyens et de prérogatives renforcés.

Vecteur : loi.

Proposition n° 42

Créer un droit de signalement à l'Autorité de contrôle des services de renseignement, l'ACSR, permettant aux agents impliqués dans la mise en œuvre des programmes de renseignement de signaler des pratiques manifestement contraires au cadre légal. Ce droit de saisine serait effectué selon des modalités sécurisées assurant la protection du secret de la défense nationale.

Vecteur : loi.

Organiser la coopération européenne et internationale (3.5.)

Affirmer l'applicabilité du droit européen et organiser la coopération au sein de l'Union européenne (3.5.1.)

Proposition n° 43

Définir un socle de règles applicables à tous les services dirigés vers l'Union européenne ou la France (selon que la règle est européenne ou nationale), quel que soit leur lieu d'établissement. Ce socle comprendrait :

- la législation européenne relative à la protection des données personnelles, qui serait qualifiée à cette fin de « *loi de police* » au sens du droit international privé.

- l'obligation de coopération des hébergeurs et des plateformes avec les autorités administratives et judiciaires, prévue par l'article 6 de la LCEN, dont le champ d'application territorial serait explicité.

- le droit pénal, qui est déjà applicable à l'ensemble des sites destinés au public français.

Vecteur : règlement de l'Union européenne pour la protection des données personnelles / loi pour l'obligation de coopération des hébergeurs et des plateformes.

Promouvoir de nouvelles formes de coopération avec les autres espaces juridiques (3.5.2.)

Proposition n° 44

Réformer le *Safe Harbor* en développant les contrôles par la *Federal Trade Commission* américaine (FTC) ou des organismes accrédités par elle, en prévoyant un droit de regard des autorités européennes sur ces contrôles et en renforçant les obligations de fond.

Vecteur : décision de la Commission européenne.

Proposition n° 45

Prévoir que les transferts de données personnelles vers certains État tiers, lorsqu'ils sont requis par les autorités administratives ou judiciaires de cet État, sont subordonnés à l'autorisation préalable de l'autorité de contrôle compétente. La décision d'appliquer ce régime à un État tiers, prise par la Commission, est temporaire et renouvelable ; elle doit être justifiée par le non-respect des standards de l'État de droit ou par le caractère excessif des pratiques de collecte de renseignement.

Vecteur : règlement de l'Union européenne.

Proposition n° 46

Subordonner la reconnaissance par l'UE du caractère adéquat de la protection dans des États tiers à une condition de réciprocité.

Vecteur : action de la Commission européenne

Proposition n° 47

Créer un groupe d'action interétatique, sur le modèle du Groupe d'action financière (GAFI), pour définir des recommandations en matière de lutte contre la cybercriminalité et publier une liste d'États non coopératifs.

Vecteur : action du Conseil de l'Europe

Rééquilibrer la gouvernance d'internet (3.5.3.)

Proposition n° 48

Promouvoir la démocratisation de l'ICANN, en :

- créant une assemblée générale rassemblant l'ensemble des parties prenantes et pouvant mettre en cause la responsabilité du conseil d'administration ;

- renforçant les mécanismes de recours internes, par exemple en dotant d'une portée contraignante le mécanisme d'*Independent Review Panel* ;

- permettant au comité représentant les gouvernements (GAC) d'adopter des résolutions contraignantes.

Vecteur : modification des statuts de l'ICANN.

Proposition n° 49

Diversifier la composition des instances de gouvernance d'internet, par des critères de sélection imposant une réelle diversité linguistique et géographique et la mise en place de stratégies d'influence au niveau de la France et de l'Union européenne.

Vecteur : modification des statuts de ces instances, action du Gouvernement français et de l'Union européenne.

Proposition n° 50

Promouvoir l'adoption d'une convention internationale relative aux libertés fondamentales et aux principes de la gouvernance d'internet.

Vecteur : convention internationale.

,

Annexes

Annexe 1 – **Liste des personnes auditionnées**

Annexe 2 – **« Groupe de contact » de l'étude annuelle : constitution et composition**

Annexe 3 – **Numérique et santé**

Annexe 4 – **Numérique et éducation**

Annexe 5 – **Numérique et relations du travail**

Annexe 1 – Liste des personnes auditionnées

Les fonctions mentionnées sont celles exercées au moment de l'audition.
Sauf indication contraire, les auditions ont eu lieu au Conseil d'État

Personne auditionnée	date
M. Thomas ANDRIEU, *directeur des libertés publiques et des affaires juridiques au ministère de l'intérieur*	30 juin 2014
Mme Maryse ARTIGUELONG, *responsable du groupe «Liberté et technologies de l'information et de la communication», Ligue des Droits de l'Homme*	7 octobre 2013
M. Jan Philipp ALBRECHT, *député européen, groupe des Verts/ Alliance libre européenne*	14 avril 2014
M. Gilles BABINET, *multi-entrepreneur, «Digital Champion», responsable des enjeux du numérique pour la France auprès de la Commission européenne*	2 décembre 2013
M. Bernard BAJOLET, *directeur général de la sécurité extérieure, DGSE*	3 décembre 2013
M. Fabrice BAKHOUCHE, *conseiller technique pour la communication et l'économie numérique au cabinet du Premier ministre*	26 novembre 2013
M. Claude BALAND, *préfet, directeur général de la police nationale*	25 mars 2014
M. Alain BAZOT, *président de l'Union fédérale des consommateurs-Que choisir ?* **Mme Amal TALEB,** *juriste «Concurrence - Nouvelles Technologies», département juridique - Union Fédérale des Consommateurs-Que choisir ?*	8 octobre 2013
M. Pierre BELLANGER, *fondateur et PDG de Skyrock, et du réseau social «Skyrock.com»*	6 mai 2014
M. Bernard BENHAMOU, *délégué aux usages de l'internet, ministère chargé des PME, de l'innovation et de l'économie numérique*	10 septembre 2013
M. Alain BENSOUSSAN, *avocat à la cour d'appel de Paris*	25 septembre 2013
Mme Thérèse BLANCHET, *directrice «justice et affaires intérieures» au service juridique du Conseil de l'Union européenne*	12 décembre 2013, Conseil de l'Union européenne

M. Jean-Claude BONICHOT, *conseiller d'État, juge à la Cour de justice de l'Union européenne (CJUE)*	14 mai 2014
Mme Marie-Hélène BOULANGER, *chef de l'unité «Protection des données», accompagnée de M. Nicolas DUBOIS, «Réforme de la protection des données»*	12 décembre 2013, Commission européenne
M. Didier CASAS, *secrétaire général de Bouygues Telecom*	3 avril 2014
M. Antonio CASILLI, *sociologue, maître de conférences en «digital humanities» à Telecom ParisTech et chercheur au Centre Edgar-Morin (EHESS)*	11 octobre 2013
Mme Carole CHAMPALAUNE, *directrice des affaires civiles et du sceau, ministère de la justice*	3 septembre 2013
M. Nicolas COLIN, *inspecteur des finances, entrepreneur*	18 septembre 2013
M. Pierre COLLIN, *conseiller d'État*	12 septembre 2013
M. Bertrand de la CHAPELLE, *membre du Board d'ICANN, ancien ambassadeur thématique pour la société de l'information au ministère des affaires étrangères*	8 novembre 2013
Mme Laure de LA RAUDIERE, *députée d'Eure-et-Loir*	19 mars 2014
M. Francis DONNAT, *Senior Policy Counsel, Google France*	9 octobre 2013
Mme Isabelle FALQUE-PIERROTIN, *présidente de la CNIL*	23 juillet 2013 et 11 juin 2014
Mme Bénédicte FAUVARQUE-COSSON, *professeur à l'université Panthéon-Assas (Paris II)*	4 juillet 2014
Mme Christiane FERAL-SCHUHL, *avocat à la Cour, ancien bâtonnier de Paris*	4 juillet 2014
Mme Laurence FRANCHESCHINI, *directrice générale des médias et des industries culturelles au ministère de la culture et de la communication*	8 avril 2014
M. Edouard GEFFRAY, *secrétaire général de la CNIL*	8 janvier 2014 et 11 juin 2014
M. Paul-Olivier GIBERT, *président de l'AFCDP (Association française des correspondants à la protection des données à caractère personnel)*	3 février 2014

M. Laurent GILLE, *chef du département Sciences économiques et sociales à Telecom ParisTech*	8 octobre 2013
M. Marco GIORELLO, *chef d'unité adjoint «Droit d'auteur» à la direction générale Marché intérieur de la Commission européenne*	12 décembre 2013, Commission européenne
M. Mathieu GUERLAIN, *conseiller technique en charge de la modernisation de l'action publique au cabinet du Premier Ministre*	26 novembre 2013
M. Dominique GUIBERT, *vice-président de la Ligue des Droits de l'Homme*	7 octobre 2013
M. Peter HUSTINX, *contrôleur européen de la protection des données – Autorité indépendante auprès des institutions et organes européens*	12 décembre 2013, Commission européenne
Mme Mireille IMBERT-QUARETTA, *présidente de la commission de protection des droits de l'Hadopi*	28 octobre 2013
M. Daniel KAPLAN, *délégué général de la Fondation Internet nouvelle génération (FING)*	2 octobre 2013
M. Thibault KLEINER, *conseiller au cabinet de Mme Neelie KROES, commissaire en charge de l'agenda numérique*	12 décembre 2013, Commission européenne
M. Hannes KRAEMER, *responsable au service juridique de la Commission européenne, accompagné de M. Bernd MARTENCZUK et de Mme Anna MARCOULLI*	12 décembre 2013, Commission européenne
Mme Claire LANDAIS, *directrice des affaires juridiques au ministère de la Défense*	19 décembre 2013 et 30 juin 2014
M. Bruno LASSERRE, *président de l'Autorité de la concurrence*	2 mai 2014
M. Hubert LEGAL, *jurisconsulte du Conseil de l'Union européenne*	12 décembre 2013, Conseil de l'Union européenne
Mme Sophie-Justine LIEBER, *conseillère en charge du numérique et des droits d'auteur au cabinet de la ministre de la culture et de la communication*	8 avril 2014
M. Jean MAFART, *chef de service à la direction générale de la sécurité intérieure*	2 juillet 2014
M. Jean-Claude MALLET, *conseiller d'État, conseiller du ministre de la Défense*	30 juin 2014
M. Cédric MANARA, *docteur en droit, professeur permanent pour l'EDHEC Business School*	19 septembre 2013

M. David MARTINON, *ambassadeur sur la société de l'information et le développement numérique*	7 février 2014
M. Winston J. MAXWELL, *avocat aux barreaux de Paris et de New York au cabinet Hogan Lovells (Paris)*	28 octobre 2013
M. Pierre-Antoine MOLINA, *directeur des libertés publiques et de l'action juridique au ministère de l'intérieur*	10 février 2014
M. Marc MOSSÉ, *directeur des affaires juridiques et des affaires publiques, Microsoft France*	25 septembre 2013
M. Patrick PAILLOUX, *directeur général de l'ANSSI (Agence nationale de la sécurité des systèmes d'information)*	28 janvier 2014
M. Christian PAUL, *député de la Nièvre, co-président du groupe d'étude « Internet et société numérique »*	25 mars 2014, Assemblée nationale
M. Hervé PELLETIER, *président de la Commission nationale de contrôle des interceptions de sécurité (CNCIS)* **M. Olivier GUERIN,** *délégué général de la Commission nationale de contrôle des interceptions de sécurité (CNCIS)*	14 mars 2014
M. Jean-Emmanuel RAY, *professeur de droit privé à Paris I (Panthéon-Sorbonne) et à Sciences Po*	16 décembre 2013
M. Maurice RONAI, *chercheur à l'École des hautes études en sciences sociales (EHESS), membre de la CNIL*	1er avril 2014
Mme Antoinette ROUVROY, *docteur en droit, spécialiste de la gouvernementalité algorithmique et membre du Comité de prospective de la CNIL*	14 avril 2014
M. Olivier SCHRAMECK, *président du Conseil Supérieur de l'Audiovisuel (CSA)*	7 octobre 2013 et 10 juin 2014, CSA
M. Vihan SHARMA, *directeur général France de Acxiom – France,* **Mme Sarah WANQUET,** *directeur juridique, Privacy Officer, Acxiom - France*	13 juin 2014
M. Jean-Ludovic SILICANI, *président de l'Autorité de régulation des communications électroniques et des postes (ARCEP)*	22 juillet 2013 et 11 juin 2014
M. Sébastien SORIANO, *directeur de cabinet de la ministre déléguée chargée des petites et moyennes entreprises, de l'innovation et de l'économie numérique*	13 mars 2014
M. Jean-Baptiste SOUFRON, *secrétaire général du Conseil National du Numérique*	30 octobre 2013

M. Bernard STIEGLER, *directeur de l'Institut de recherche et d'innovation*	13 novembre 2013
M. Jean-Pierre SUEUR, *sénateur du Loiret, président de la commission des lois du Sénat*	18 mars 2014, Sénat
M. Benoît THIEULIN, *président du Conseil national du numérique (CNN)*	30 octobre 2013
M. Thierry TUOT, *conseiller d'État, président de sous-section*	18 juillet 2013
M. Jean-Jacques URVOAS, *député du Finistère, président de la commission des lois de l'Assemblée nationale*	1er avril 2014 Assemblée nationale
M. Henri VERDIER, *directeur d'Etalab*	2 octobre 2013 et 27 mars 2014
M. Mathieu WEILL, *directeur général de l'Association française pour le nommage internet en coopération (AFNIC)*	24 juillet 2013 et 23 mai 2014
M. Thierry ZYLBERBERG, *vice-président d'Orange-Santé*	16 juin 2014
M. Jérémie ZIMMERMANN, *fondateur et ex-porte-parole de l'association La Quadrature du Net*	28 janvier 2014

En outre, le président de la SRE, le rapporteur général et le rapporteur général adjoint ont été auditionnés par :

■ la mission commune d'information sur le nouveau rôle et la nouvelle stratégie de l'Union européenne dans la gouvernance mondiale de l'internet, présidée par M. Gaëtan GORCE (sénateur de la Nièvre) – Rapporteur : Mme Catherine MORIN-DESAILLY (sénatrice de la Seine-Maritime) – 8 avril 2014 au Sénat.

■ la mission d'information de la commission des lois sur « l'*open data* » – M. Gaëtan GORCE (sénateur de la Nièvre) et François PILLET (sénateur du Cher), co-rapporteurs – 9 avril 2014 au Sénat.

De plus, des informations complémentaires ont été recueillies dans deux cadres particuliers.

■ Une matinée de travail a eu lieu au pôle judiciaire de la gendarmerie nationale (fort de Rosny-sous-Bois) le 15 avril 2014 organisée par le Général Jacques HEBRARD : avec notamment quatre ateliers à la division «lutte contre la cybercriminalité» (enquête sous pseudonymes, expérimentation sur les réseaux sociaux, recherches d'images et vidéos similaires, investigation sur internet à partir d'un nom ou d'une adresse), un atelier à la division «informatique-électronique» et un atelier au service technique de recherche judiciaire et de documentation.

■ Un panel de « correspondants informatiques et libertés » (CIL appartenant à l'Association française des correspondants à la protection des données à caractère personnel (AFCDP) a été consulté le 15 mai 2014. Il était composé de :

M. Paul-Olivier GIBERT, président de l'AFCDP et président fondateur du cabinet Digital et Ethics

M. Sylvain BONENFANT, CIL du conseil général de Seine-Maritime

Mme Pascale GELLY, avocate (cabinet GELLY)

Mme Daphné JAYET, CIL au centre hospitalier d'Arras (Pas de Calais)

M. Xavier LECLERC, CIL mutualisé cabinet AnaXil

Mme RICONART-MALLET, avocate au cabinet BRM (Nord)

M. Philippe SALAÜN, CIL groupe CNP-assurances

M. Stéphane SCHMOLL, CIL, président de la *start up* DEVERY WARE

Mme Marie-Noëlle SEHABIAGUE, CIL CNAF Paris

Annexe 2 – « Groupe de contacts » de l'étude annuelle : constitution et composition

Le « groupe de contacts » constitué dans le cadre des travaux d'élaboration de l'étude annuelle 2014 du Conseil d'État a eu pour rôle de discuter et mettre en débat les orientations que les rédacteurs chargés de l'étude, au fur et à mesure de leurs investigations et auditions, ont été en mesure de proposer.

Il s'agissait moins d'un groupe de travail que d'un comité scientifique informel, dont la qualification et la légitimité résultaient de la bonne connaissance du « milieu » du numérique et de ses usages dont ses membres disposent. La perception et la compréhension des enjeux de la société de l'information, telle que façonnée par la généralisation des technologies numériques, ont nourri les échanges très utiles aux rédacteurs de l'étude et aux délibérations de la Section du rapport et des études du Conseil d'État.

Le groupe s'est réuni à quatre reprises pendant la durée de l'élaboration de l'étude : le 13 novembre 2013, le 14 mars 2014, le 19 mai 2014 et le 23 juin 2014.

La composition du groupe, constitué d'une vingtaine de personnalités, a permis d'assurer la diversité et la complémentarité des expressions dans un domaine, par nature, composite et propice au débat d'idées entre les différents groupes d'intérêts réunis en la circonstance.

Composition

Maryse ARTIGUELONG, *responsable du groupe de travail « Libertés et Technologies de l'information et de la communication » à la Ligue des droits de l'Homme,*

Christine BALAGUE, *vice-présidente « Libertés et droits fondamentaux », du Conseil national du numérique (CNN),*

Bernard BENHAMOU, *délégué aux usages de l'internet au ministère chargé des PME, de l'Innovation et de l'Economie numérique,*

Alain BENSOUSSAN, *avocat à la Cour, AB Avocats,*

Antonio CASILLI, *sociologue, maître de conférences en digital humanities à Telecom ParisTech et chercheur au Centre Edgar-Morin (EHESS),*

Nicolas COLIN, *inspecteur des finances, entrepreneur, co-auteur du rapport sur la fiscalité du numérique avec Pierre Collin,*

David EL SAYEGH, *délégué général de la Société des auteurs, compositeurs et éditeurs de musique (SACEM),*

Nelly FESSEAU, *directrice-adjointe chargée de la formation permanente à l'Ecole nationale d'administration ; co-auteure de « Numérique, renouer avec les valeurs progressistes et dynamiser la croissance » avec Gabriel Lavenir*,

Edouard GEFFRAY, *secrétaire général de la CNIL,*

Jean-Baptiste GOURDIN, *directeur du cabinet du Président du Conseil supérieur de l'audiovisuel (CSA),*

Stéphane HOYNCK, *directeur général adjoint de l'ARCEP,*

Bertrand de LA CHAPELLE, *ambassadeur thématique pour la gouvernance internet de 2006 à 2010 ; directeur de programmes à l'Académie diplomatique internationale, membre du board directeur ICANN,*

Cédric MANARA, *docteur en droit, professeur permanent par l'EDHEC Business School. En charge de la rubrique « Commerce électronique » du Recueil Dalloz,*

Jacques MARZIN, *directeur de la direction interministérielle des systèmes d'information et de communication de l'État (Secrétariat général pour la modernisation de l'État),*

Marc MOSSÉ, *directeur des affaires juridiques et des affaires publiques de Microsoft France,*

Bernard STIEGLER, *directeur de l'Institut de recherche et d'innovation (IRI), au sein du Centre Georges-Pompidou,*

Amal TALEB, *responsable du pôle « concurrence, nouvelles technologies », département juridique de l'Union fédérale des consommateurs – Que choisir ?,*

Jean-Marc TASSETTO, *ancien directeur général de Google France, créateur d'une société d'e-learning.*

Annexe 3 – Numérique et santé

Le développement du numérique dans le domaine de la santé est à la fois un atout pour le système de santé et un risque pour les droits et libertés fondamentaux consacrés dans ce champ. Il a nécessité la mise en place d'un cadre juridique particulièrement protecteur des données personnelles de santé (I) et fait émerger de nouveaux débats appelant des réponses audacieuses (II).

I. La mise en place d'un cadre juridique protecteur pour les données personnelles relatives à la santé

Le législateur s'est saisi dès 1978 de la problématique des *«données à caractère personnel»*[1] et en 2004, sous l'impulsion de l'Union européenne, de celle, plus particulière, des *« données à caractère personnel relatives à la santé des personnes »*[2]. Cette reconnaissance de la sensibilité des données relatives à la santé a justifié l'introduction de dispositions régissant de manière générale leur collecte et leur traitement (A) et de dispositions particulières complémentaires (B).

A. L'introduction de dispositions régissant la collecte et le traitement des données de santé à caractère personnel

Après avoir rappelé les fondements juridiques justifiant une protection spécifique des données de santé (1), on évoquera les dispositions de la loi de 1978 dite « informatique et libertés », révisée en 2004, qui régissent leur collecte et leur traitement (2).

1. Les fondements juridiques d'une protection spécifique des données de santé

a) Le droit au respect de la vie privée

Le droit au respect de la vie privée, énoncé à l'article 2 de la DDHC[3], à l'article 8 de la Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales et à l'article 9 du code civil (C. Civ.) justifie une protection spécifique des données de santé. L'article 1er de la loi « informatique et libertés » rappelle ce principe et la directive communautaire de 1995, transposée par la loi de 2004, prescrit aux États membres d'assurer la protection de la vie privée des personnes physiques par une règlementation adaptée du traitement des données à caractère personnel. Dans le domaine de la santé, ce nécessaire respect du droit à la vie privée est rappelé à l'article L. 1110-4 du code de la santé, qui dispose *que « toute personne prise en charge par un professionnel, un établissement, un réseau de*

1. Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

2. Loi n° 2004-801 du 6 août 2004 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel et modifiant la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, transposant la directive 95/46/CE du Parlement européen et du Conseil relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données.

3. CC, décision n° 99-416 DC du 23 juillet 1999, *Loi portant création d'une couverture maladie universelle*.

santé, ou tout autre organisme participant à la prévention et aux soins a droit au respect de sa vie privée, et du secret des informations la concernant ». Par ailleurs, la jurisprudence invoque souvent ce droit à la vie privée en matière de santé[4]. Enfin, le code pénal (C. Pén.) sanctionne ces atteintes à la vie privée dans le domaine de la santé (226-15 C. Pén. pour l'atteinte au secret des correspondances ; 226-22 C. Pén. pour la divulgation de données à caractère personnel par la personne qui les a recueillies).

b) La protection par le secret médical

Par ailleurs, les informations médicales concernant la personne, *« venues à la connaissance du professionnel de santé, de tout membre du personnel de ces établissements ou organismes et de toute autre personne en relation, de par ses activités, avec ces établissements ou organismes »* sont protégées par le secret médical (L.1110-4 du Code de la santé publique (CSP)). Dans le même sens, est sanctionnée *« la révélation d'une information à caractère secret par une personne qui est dépositaire soit par état ou par profession, soit en raison d'une fonction ou d'une mission temporaire »* (226-13 C. Pén.) étant précisé que le secret médical est une composante du secret professionnel[5]. Les professionnels de santé peuvent également être poursuivis à titre disciplinaire sur le fondement des codes de déontologie applicables à leur profession[6]. Cependant la loi de 2002 relative aux droits des malades et à la protection du système de santé[7] autorise le partage des informations entre médecins participant aux soins d'un même patient (L. 1110-4 CSP).

2. Les dispositions de la loi « Informatique et Libertés » applicables à la collecte et au traitement des données de santé

a) La collecte et le traitement des données personnelles de santé : un principe d'interdiction du traitement des données de santé assorti de dérogations

En vertu de la loi « Informatique et Libertés » révisée, *« il est interdit de collecter ou de traiter des données à caractère personnel […] qui sont relatives à la santé. »* (article 8-I). De même, la Convention du Conseil de l'Europe du 28 janvier 1981 instaurait déjà des *« catégories particulières de données »,* parmi lesquelles les *« données à caractère personnel relatives à la santé »,* dont le traitement était interdit, sauf *« garanties appropriées* ». Cette interdiction est pénalement sanctionnée par l'article 226-19 du code pénal.

Ce principe d'interdiction est tempéré par plusieurs dérogations (article 8-II et suivants). Les premières sont directement issues de la directive et reprises par le droit français. Ainsi en est-il du consentement exprès de la personne concernée,

4. Cass., Soc., 10 juillet 2002, Bull. civ., V, n° 251 ; Cass., 2ème civ., 19 février 2009, Bull. Civ., II, n° 62.

5. Cass., Crim., 30 janvier 2001, n° 00-81-309 ; Cass., 1ère civ., 14 décembre 1999, n° 97-15-756.

6. CE, 29 décembre 2000*, M. Gubler*, n° 212440 ; CE, 28 mai 1999, *M. Tordjemann*, n° 189057.

7. Loi n° 2002-303 du 4 mars 2002 relative aux droits des malades et à la qualité du système de santé.

des traitements nécessaires à la sauvegarde de la vie humaine, mais auxquels la personne concernée ne peut donner son consentement par suite d'une incapacité juridique ou d'une impossibilité matérielle, des traitements portant sur des données à caractère personnel rendues publiques par la personne concernée, des traitements nécessaires aux fins de la médecine préventive des diagnostics médicaux de l'administration de soins ou de traitements, de la gestion des services de santé mis en œuvre par un membre d'une profession de santé ou par une autre personne à laquelle s'impose en raison de ses fonctions l'obligation de secret professionnel prévue par l'article 226-13 du code pénal, des traitements automatisés ou non, justifiés par l'intérêt public. Les secondes sont spécifiques au droit français[8]. Il en va ainsi des traitements nécessaires à la recherche dans le domaine de la santé ou de certains traitements autorisés par la Commission nationale de l'informatique et des libertés (CNIL), lorsque les données traitées sont appelées à faire l'objet à bref délai d'un procédé d'anonymisation préalablement reconnu conforme.

b) Les dispositions spécifiques à la recherche dans le domaine de la santé et à l'évaluation et à l'analyse des activités de soin.

• La recherche dans le domaine de la santé

Le chapitre IX de la loi « informatique et libertés », issu d'une des lois de bioéthique de 1994, énonce les dispositions spécifiques à la recherche dans le domaine de la santé. La formalité préalable s'articule en deux phases successives : l'avis du comité consultatif sur le traitement de l'information en matière de recherche dans le domaine de la santé, institué auprès du ministre chargé de la recherche et l'avis de la CNIL. Le secret médical est aménagé, puisque *« les membres des professions de santé peuvent transmettre les données à caractère personnel qu'ils détiennent »* dans ce cadre. Cependant, *« lorsque ces données permettent l'identification des personnes, elles doivent être codées avant leur transmission* ». En tout état de cause, *« la présentation des résultats des données ne peut en aucun cas permettre l'identification directe ou indirecte des personnes concernées »* (article 55). Le consentement du patient reste déterminant. Ainsi, les patients ont le droit de s'opposer à ce que les informations nominatives les concernant fassent l'objet d'un traitement (article 56) et toute personne a le droit de s'opposer à ce que des données à caractère personnel la concernant fassent l'objet de la levée du secret professionnel rendue nécessaire par un traitement. En outre, *« dans le cas où la recherche nécessite le recueil de prélèvements biologiques identifiants, le consentement éclairé et exprès des personnes concernées »* doit être obtenu au préalable (article 56). L'obligation d'information des personnes concernées est plus poussée.

8. Tout en étant compatibles avec la directive, dont l'article 8.4 prévoit que « *sous réserve de garanties appropriées, les États membres peuvent prévoir, pour un motif d'intérêt public important, des dérogations autres que celles prévues au paragraphe 2, soit par leur législation nationale, soit sur décision de l'autorité de contrôle* ».

• L'évaluation et l'analyse des activités de soin

Le chapitre X, relatif au traitement des données personnelles de santé à des fins d'évaluation ou d'analyse des activités de soins et de prévention, a été créé à l'occasion de la loi du 27 juillet 1999 sur la couverture maladie universelle (CMU). Rédigé en vue de la mise en place du « programme de médicalisation des systèmes d'information » (PMSI) dans les hôpitaux, ce chapitre n'autorise le traitement de données de santé à cette fin que si celles-ci sont agrégées ou anonymisées. Seule la CNIL peut autoriser une dérogation à cette règle, auquel cas les données utilisées ne doivent comporter ni le nom, ni le prénom, ni le NIR (numéro d'inscription au répertoire) des personnes concernées.

B. Les régimes particuliers complémentaires applicables aux données de santé

Depuis la loi de 2002[9], la collecte et le traitement des données de santé sont régis, en complément de la loi « informatique et libertés », par des dispositions du CSP et du code de la sécurité sociale (C. Sec. Soc.), qui renvoient le plus généralement soit au respect de la loi de 1978, soit à l'avis de la CNIL. Ainsi en est-il des dispositions spécifiques à l'hébergement des données de santé, au dossier médical personnel, au dossier pharmaceutique et au web médecin (1). Par ailleurs, doit être également évoqué l'encadrement juridique des bases administratives nationales comportant des données individuelles de santé (2).

1. Les dispositions spécifiques à l'hébergement des données de santé, au dossier médical personnel, au dossier pharmaceutique et au web médecin

a) L'hébergement des données de santé

La loi de 2002 consacre la possibilité pour les professionnels de santé et les établissements de santé *de « déposer des données de santé à caractère personnel, recueillies ou produites à l'occasion des activités de prévention, de diagnostic ou de soins auprès de personnes physiques ou morales agrées à cet effet»* (L. 1111-8 CSP). Le consentement exprès de la personne concernée est requis. Ce type de traitement est soumis aux dispositions de la loi « informatique et libertés » et une procédure particulière d'agrément des hébergeurs est prévue.

b) Le dossier médical personnel (DMP), le dossier pharmaceutique (DP) et le web médecin

Le principe législatif de l'établissement d'un dossier médical personnel (DMP) a été établi en 2004 : chaque bénéficiaire de l'assurance maladie doit disposer d'un DMP et chaque professionnel de santé doit y reporter, *« à l'occasion de chaque acte ou consultation, les éléments diagnostiques et thérapeutiques nécessaires à la coordination des soins de la personne prise en charge »* (L. 1111-14 à L. 1111-24 CSP[10]). Ce DMP relève des dispositions sur l'hébergement des données de santé. L'établissement de ce dossier a connu des vicissitudes qui ne garantissent pas son extension générale (à la date de la publication de la présente étude).

9. Loi n° 2002-303 du 4 mars 2002 relative aux droits des malades et à la qualité du système de santé.

10. Loi n° 2004-810 du 13 août 2004 relative à l'assurance maladie, modifiée par la loi n° 2009-879 du 21 juillet 2009 portant réforme de l'hôpital et relative aux patients, à la santé et aux territoires.

En 2007[11] a été instituée l'obligation de créer pour chaque bénéficiaire de l'assurance maladie un dossier pharmaceutique (DP) qui devait alimenter le dossier médical personnel. À la différence de ce dernier, il a pu se généraliser sans difficulté particulière et il permet l'accès à l'historique des médicaments qui ont été délivrés au patient durant les quatre derniers mois. Si la constitution d'un DMP pour chaque patient sera à terme obligatoire, la création du DP se fait avec le consentement du patient. Les pharmaciens doivent alimenter le dossier lors de la délivrance du médicament. Toutefois, les patients peuvent s'opposer à l'alimentation ou à l'accès au dossier.

Enfin, la CNAM a mis en place à partir de 2006 le « *web* médecin »[12]. Ce service permet aux praticiens libéraux de prendre connaissance de l'ensemble des soins, médicaments et examens qui ont été prescrits et remboursés à leurs patients par l'assurance maladie au cours des douze derniers mois. L'accès à cet outil se fait via la carte professionnelle du médecin et la carte Vitale du patient, qui doit donner son accord pour la consultation des données qui le concernent.

2. Les bases administratives nationales comportant des données individuelles de santé

a) Les principales bases existantes : le programme de médicalisation des systèmes d'information (PMSI), le système national d'information inter-régimes de l'assurance maladie (SNIIRAM) et les informations sur les décès

Mis en place en 1996, le PMSI rassemble des informations quantifiées et standardisées afin de mesurer l'activité et les ressources des établissements de santé. On y retrouve des informations sur les patients reçus dans l'ensemble des établissements sanitaires telles que le motif médical d'entrée, les actes médicaux pris en charge, la durée de séjour ou encore le mode de sortie. Cette base est gérée par l'Agence technique de l'information sur l'hospitalisation (ATIH), qui en transmet depuis 2007 une copie au SNIIRAM.

Créé en 1998[13] et mis en place progressivement depuis 2004, le SNIIRAM contient le détail des remboursements de soins aux malades français effectués par les caisses d'assurance maladie et des références sur les assurés, les professionnels et les établissements de santé, ainsi que les employeurs. Géré par la CNAM, il contient donc des données sur les patients (âge, sexe, département et région de résidence, date de décès) et sur la consommation de soins en ville, avec le détail par date de soins et date de remboursement de toutes les prestations remboursées et le codage détaillé de la prestation.

---

11. Loi n° 2007-127 du 30 janvier 2007 ratifiant l'ordonnance n° 2005-1040 du 26 août 2005 relative à l'organisation de certaines professions de santé et à la répression de l'usurpation de titres et de l'exercice illégal de ces professions et modifiant le code de la santé publique, intégrant dans le code de sécurité sociale un article L. 161-16-4-2, déplacé par la loi n°2009-879 du 21 juillet 2009 dite « HPST » à l'article L. 1111-23 du code de la santé publique.

12. Décret n° 2006-143 du 9 février 2006 relatif aux modalités d'accès des médecins aux données relatives aux prestations servies aux bénéficiaires de l'assurance maladie et modifiant le code de la sécurité sociale.

13. Loi n° 98-1194 du 23 décembre 1998 de financement de la sécurité sociale pour 1999.

Le répertoire national d'identification des personnes physiques (RNIPP) géré par l'INSEE et son miroir à la CNAV, le système national de gestion des identités (SNGI), comportent en plus des éléments sur l'identité et la santé des personnes qu'ils fournissent aux organismes de sécurité sociale.

Le centre d'épidémiologie sur les causes médicales de décès (CépiDc) est un laboratoire de l'INSERM, destinataire de la partie médicale des certificats de décès, lesquels font l'objet d'un appariement avec le SNIIRAM.

b) Les restrictions juridiques à l'accès au système d'information

L'entrepôt de données du SNIIRAM n'est pas fait pour être interrogé directement et différentes modalités de consultation sont prévues. Ainsi, l'échantillon généraliste de bénéficiaires (EGB) est un échantillon permanent représentatif de la population protégée par l'assurance maladie, qu'elle ait ou non perçu des remboursements de soins ; il regroupe actuellement près de 500 000 bénéficiaires du régime général. Le SNIIRAM a aussi été organisé pour permettre aux personnes habilitées d'effectuer des requêtes sur le SNIIRAM en utilisant pour ce faire des « magasins » appelés *datamarts*, au nombre de seize, regroupés par thèmes (bénéficiaires, dépenses, offre de soins…). Enfin, des données peuvent en être extraites à la demande et communiquées sous certaines conditions en vue d'études spécifiques impliquant ou non l'appariement avec des données d'enquêtes ou avec les données d'une autre base administrative. Selon qu'il s'agisse de l'EGB, des données agrégées des *datamarts*, ou des extractions *ad hoc*, un nombre plus ou moins grand de personnes peuvent accéder aux données du SNIIRAM. En revanche, aucune entité poursuivant un but lucratif ne peut y accéder.

S'agissant des accès aux données du PMSI, auprès de l'Agence technique de l'information sur l'hospitalisation, seul l'accord de la CNIL est nécessaire et les organismes publics peuvent disposer des données gratuitement.

II. Les nouveaux débats de la santé à l'heure du numérique

Le développement de l' « e-santé » introduit un véritable changement de paradigme pour le système de soins. Ainsi, alors que le traitement numérique des informations sur chaque patient se généralise, la question de l'ouverture des bases administratives de données de santé se pose (A). Par ailleurs, l'utilisation des données est déterminante dans l'organisation de nouvelles formes de médecine (B).

A. La problématique de l'ouverture des bases administratives de données de santé

La France dispose de bases de données médico-sociales et économiques nationales centralisées, constituées et gérées par des organismes publics, qui couvrent de façon exhaustive et permanente l'ensemble de la population dans divers domaines stratégiques pour la santé publique et la recherche. Cependant, l'utilisation à des fins de recherche et de surveillance de ces bases de données nationales se heurte actuellement à des obstacles divers, en particulier juridiques. Ainsi, nombreux sont aujourd'hui ceux qui sollicitent une plus large ouverture de ces bases de données

de santé, en particulier du SNIIRAM élargi (1). Cependant, d'autres sont plus prudents, mettant en avant les risques résultant d'une telle ouverture de l'accès à des données particulièrement sensibles (2).

1. Les arguments en faveur d'une ouverture des bases de données de santé

a) Une volonté d'engager la réflexion sur l'ouverture des bases de données de santé

Récemment, les difficultés d'accès et la sous utilisation des données de santé ont été mises en cause. Ainsi, les chercheurs en épidémiologie, sous l'égide du professeur M. Goldberg, avaient dressé un tableau précis et critique des obstacles auxquels se heurtent les chercheurs, dans deux rapports du Haut Conseil de la santé publique (HCSP), en 2009[14] et en 2012[15]. L'Institut des données de santé (IDS) plaide régulièrement pour une ouverture des données de santé à la société civile[16]. À l'automne 2012, la direction de la recherche, des études, de l'évaluation et des statistiques (DREES) a réuni un groupe d'experts pour identifier les obstacles juridiques et techniques à l'usage des données par les chercheurs et les administrations et y proposer des solutions. Des tribunes dans la presse[17] et une pétition de janvier 2013 de l'Initiative transparence santé ont ravivé le débat. Enfin, l'avis favorable rendu en novembre 2013 par la Commission d'accès aux documents administratifs (CADA) à la demande d'accès aux données de consommation du Médiator[18] a fait l'objet d'un large écho médiatique. Dans ce contexte, la ministre de la santé M. Touraine a demandé en avril 2013 un rapport sur la gouvernance et l'utilisation des données de santé à Pierre-Louis Bras, inspecteur général des affaires sociales. Le rapport a été rendu en septembre 2013[19].

b) Les bénéfices potentiels de l'ouverture du SNIIRAM

Le rapport souligne les bénéfices potentiels de l'ouverture d'une telle base de données, du point de vue démocratique, économique et surtout sanitaire.

Les enjeux démocratiques de l'ouverture des données de santé sont liés à la thématique de l'ouverture des données publiques et de l'accès aux documents administratifs[20]. Ainsi, il s'agit d'assurer une transparence sur l'activité de l'administration et une meilleure information des citoyens administrés, pour alimenter le débat public sur les politiques publiques de santé.

Les enjeux sont également économiques en ce que l'ouverture de ces données permettrait un meilleur pilotage du système de santé et une plus grande maîtrise des dépenses de santé. On pourrait par exemple prévenir la surconsommation de

14. HCSP, *Les systèmes d'information pour la santé publique*, novembre 2009.

15. HCSP, *Pour une meilleure utilisation des bases de données médico-administratives*, mars 2012.

16. IDS, Rapport, 2011 ; IDS, Rapport, 2012.

17. J. De Kervasdoué, D. Sicard, « Plus grave que le débat sur la pilule, l'affaire des données de santé publique », *Le Monde*, 15 janvier 2013.

18. CADA, Avis n°20134348 du 21 novembre 2013.

19. P.-L. Bras, *Rapport sur la gouvernance et l'utilisation des données de santé*, septembre 2013.

20. Loi n° 78-753 du 17 juillet 1978 portant diverses mesures d'amélioration des relations entre l'administration et le public et diverses dispositions d'ordre administratif, social et fiscal.

médicaments, qui a un coût à la fois économique et humain. De plus, la disponibilité d'une telle base, dans la mesure où elle peut favoriser le développement d'une recherche publique ou privée en santé, peut constituer un atout dans la compétition internationale en matière de recherche.

Enfin, les enjeux sont surtout sanitaires. En effet, l'ouverture de cette base de données permettrait des avancées considérables en matière d'épidémiologique, en particulier quant aux études et recherches de grande dimension et de longue durée. De la même façon, cela serait particulièrement intéressant pour les études de pharmaco-épidémiologie et de suivi post-autorisation de mise sur le marché. Enfin, cela permettrait d'améliorer l'efficacité de la veille sanitaire ; c'est, en effet, l'exploitation du SNIIRAM qui a permis d'établir les risques liés au Médiator[21].

2. Les arguments contre une ouverture des bases de données de santé

a) La problématique du recueil du consentement des personnes

Dans la plupart des situations d'utilisation des données à caractère personnel des bases nationales envisagées ici, il n'est en pratique pas possible de recueillir un consentement explicite des personnes concernées avant chaque étude ou appariement systématique.

Il y a donc là une difficulté vis-à-vis de la loi « informatique et libertés », qui nécessite des dispositifs d'information acceptables par la CNIL.

b) Le risque de réidentification et de mésusage des données

Pour Pierre-Louis Bras, l'utilisation des bases constituées à partir de données de santé individuelles, pour des finalités collectives d'études ou de recherches, ne doit pas remettre en cause le droit des personnes au respect de leur vie privée[22]. Il *« doit donc être admis que si des données de santé sont directement ou indirectement nominatives, l'accès doit en être restreint ou contrôlé ».* Or il constate un risque de réidentification des personnes dans cette base pourtant réputée anonyme. Ainsi, si les données individuelles détaillées du SI sont bien anonymes prises une par une, le croisement de certaines informations qui y figurent permet d'identifier des personnes connues par ailleurs.

Outre ce risque de réidentification, le rapport « Bras » souligne un risque de *« mésusage des données »* par la diffusion, intentionnelle ou non, d'informations biaisées. En effet, les données ne valent que par l'interprétation qui en est fournie. Les données brutes peuvent ainsi être trompeuses, et lorsqu'elles sont traitées, il faut prendre en compte la subjectivité du résultat.

B. La nécessité d'appréhender l'émergence de nouvelles formes de médecine

Le numérique fait émerger de nouvelles façons de pratiquer la médecine et d'y avoir accès. Il faut cependant distinguer la télémédecine, dont la seule novation

21. A. Weill, M. Païta, P. Tuppin, J.-P. Fagot, A. Neumann, et al., *Benfluorex and valvular heart disease: a cohort study of a million people with diabetes mellitus,* Pharmacoepidemiol Drug Saf, 2010, 19: 1256–1262.
22. CC, décision n° 99-416 DC du 23 juillet 1999, *Loi portant création d'une couverture maladie universelle*.

est la pratique à distance grâce aux nouvelles technologies de l'information et de la communication (1), des nouveaux dispositifs permettant au patient d'être acteur de sa santé, le cas échéant sans recours à un professionnel médical (2).

1. La médecine à distance : une réponse organisationnelle et technique potentielle aux nouveaux défis de notre système de santé

a) L'élaboration d'un cadre juridique pour la télémédecine

Conscient des défis auxquels est confronté notre système de santé, en termes d'épidémiologie (augmentation du nombre de patients souffrant de maladies chroniques et/ou de poly-pathologies liées au vieillissement de la population), de démographie des professionnels de santé (inégale répartition des professionnels sur le territoire national) et de contrainte budgétaire, le législateur a entendu consacrer la télémédecine[23] en définissant son cadre juridique[24]. L'article L. 6316-1 du CSP la définit comme « une *forme de pratique médicale à distance utilisant les technologies de l'information et de la communication »,* qui *« met en rapport, entre eux ou avec un patient, un ou plusieurs professionnels de santé, parmi lesquels figure nécessairement un professionnel médical et, le cas échéant, d'autres professionnels apportant leurs soins au patient*, et *« permet d'établir un diagnostic, d'assurer, pour un patient à risque, un suivi à visée préventive ou un suivi post-thérapeutique, de requérir un avis spécialisé, de préparer une décision thérapeutique, de prescrire des produits, de prescrire ou de réaliser des prestations ou des actes, ou d'effectuer une surveillance de l'état des patients »*.

Au vu de ces différents éléments, cinq types d'actes ont été définis par décret (R. 6316-1[25]) : la téléconsultation, la téléexpertise, la télésurveillance médicale, la téléassistance médicale ainsi que la réponse médicale qui est apportée dans le cadre de la régulation médicale téléphonique des activités de permanence des soins et d'aide médicale urgente.

b) Les enjeux de la télémédecine

En dépit de sa consécration législative, de nombreuses questions se posent aujourd'hui quant à l'avenir de la télémédecine.

• La question du financement de la télémédecine

Tout d'abord, le développement de la télémédecine pose la question de son financement. Il faut distinguer à cet égard le remboursement des actes de télémédecine (tarification des actes) et le financement de l'organisation de l'activité de télémédecine.

Le décret de 2010 prévoit que la rémunération et le remboursement des actes s'organisent conformément aux dispositions du code de la sécurité sociale et dépendent de leur inscription à la classification commune des actes médicaux

23. Loi n° 2004-810 du 13 août 2004 relative à l'assurance maladie.

24. Loi n°2009-879 du 21 juillet 2009 portant réforme de l'hôpital et relative aux patients, à la santé et aux territoires.

25. Décret n° 2010-1229 du 19 octobre 2010 relatif à la télémédecine.

(CCAM). Les actes de télémédecine ne sont donc actuellement pas remboursés en tant que tels par l'Assurance maladie. Par ailleurs, ce texte précise que *« l'activité de télémédecine peut bénéficier des financements »* du Fonds d'intervention pour la coordination et la qualité des soins (FICQS) ou de la dotation des Missions d'intérêt général et d'aide à la contractualisation (MIGAC), ainsi que de dotations de l'État et des départements aux établissements sociaux et médico-sociaux. Si ces financements sont encouragés, ils ne sont pas automatiques.

• Une nouvelle forme d'exercice de la médecine multipliant les cas de responsabilité

Le développement de la télémédecine est une prise en charge collective du patient et fait intervenir un nouvel intervenant, le tiers technologique, aussi appelé prestataire technique. Néanmoins elle ne relève pas d'un régime de responsabilité spécifique de sorte que c'est le droit commun de la responsabilité civile qui trouve à s'appliquer. Dans ce cadre, la détermination des responsabilités des différents intervenants dans le préjudice engendré par l'acte de télémédecine peut se révéler délicate.

2. Le patient, acteur de sa santé : quelles conséquences pour la confidentialité des données de santé ?

a) Le succès des sites d'informations médicales

L'information de l'internaute en matière de santé se développe, avec des sites proposant *« sous la forme de dossiers thématiques, d'encyclopédies médicales, de guides de médicaments, de rubriques d'actualité, des informations pratiques portant non seulement sur la santé, mais également sur des thèmes tel que la nutrition, la sexualité, ou encore la beauté, la forme et la psychologie* »[26]. Or les éditeurs de site peuvent fournir *« des données fantaisistes, trompeuses, voire illicites au regard du droit français »*[27] en tant qu'ils entrent dans le champ de l'exercice illégal de la médecine (L. 4161-1 CSP). Des normes déontologiques encadrent ces sites d'informations médicales, notamment afin de garantir la qualité de l'information offerte au public (R. 4127-13 et suivants CSP).

Par ailleurs, la loi de 2004 relative à l'assurance maladie, modifiée en 2007, a créé la Haute Autorité de Santé (HAS), notamment chargée d'établir *« une procédure de certification des sites informatiques dédiés à la santé, et des logiciels d'aide à la prescription médicale ayant respecté un ensemble de règles de bonnes pratiques »* (article L. 161-38 du code de la Sécurité sociale). La certification « *Hon* » (« *Health on the internet »*), accréditée par la HAS[28], ne garantit pas le contenu du site, mais traduit l'engagement de l'éditeur du site à respecter des principes de transparence et à diffuser de l'information de santé répondant à certains critères de qualité.

26. CNIL, Rapport pour 2000, p. 135.

27. M. Harichaux, Internet et santé publique, Limites du droit, in Drôle(s) de droit(s), *Mélanges en l'honneur d'Elie Alfarandi*, D. 2000, p. 275.

28. HAS, Décision n°2007.11.040/DCI, 7 novembre 2007.

b) Les réseaux sociaux, lieux de discussion autour de la santé

Les réseaux sociaux généralistes offrent de nombreuses informations relatives à la santé. Ainsi, selon le baromètre « Web et Santé » (*Hopscotch* / *Listening Pharma*), *Facebook* représente 51% des conversations sur le thème de la santé. Certains ont voulu exploiter ce potentiel en développant des initiatives qui illustrent les potentialités et les dangers du partage d'informations relatives à la santé sur les réseaux sociaux. Ainsi, une application *« Help, I Have the Flu »* utilise et analyse les statuts *Facebook* des amis, afin d'alerter l'utilisateur sur l'état de santé de ses amis. Plus sérieusement, des chercheurs de l'université de Rochester se sont intéressés aux échanges postés sur *Twitter* par les utilisateurs malades, afin de mettre au point une application appelée *GermTracker*, dont l'algorithme est capable de cartographier dans l'espace et dans le temps les lieux où les maladies sont les plus actives.

Par ailleurs, les réseaux sociaux dédiés à la santé se multiplient. Ce sont tout d'abord des réseaux entre patients qui mettent en relation des patients ou leurs proches afin de faciliter le partage d'expériences et d'informations. Leur intérêt croit en fonction du nombre de leurs membres, qui reste limité en France. Un bon exemple des enjeux du développement de ce type de réseaux est donné par *patientlikeme.com*, communauté de patients atteints de différentes maladies chroniques (notamment des maladies rares) créée en 2004, aux États-Unis, par trois ingénieurs du MIT. Les patients y enregistrent et partagent des informations personnelles telles que l'âge, le sexe, l'état de santé général, mais aussi le contenu de leur dossier médical, incluant les diagnostics reçus, les traitements prescrits et leurs effets observés. Ils peuvent ainsi se comparer à d'autres patients atteints de la même maladie et ayant un profil similaire. Cela construit une base de données très riche compte tenu du nombre élevé de membres (200 000 en 2013, couvrant 1500 maladies), qui est exploitée par les administrateurs du site en partenariat avec des compagnies pharmaceutiques partenaires du projet. Ceux-ci y voient une alternative aux coûteux essais cliniques réalisés après la commercialisation d'un médicament.

Les réseaux permettant aux seuls professionnels de santé d'échanger et de partager l'information sur leurs patients (*Talent Pharmacie, MeltingDoc, DocteurSearch*) se développent également, même s'ils restent encore peu connus, puisque seulement 34% des professionnels annoncent connaître au moins un réseau social de santé. D'après l'Observatoire Santé Connect 2012, les professionnels de santé utilisent à des fins professionnelles trois fois plus souvent les réseaux sociaux généralistes que les réseaux sociaux spécialisés, ce qui peut porter atteinte à la confidentialité des informations échangées.

c) Le quantified self et les objets connectés

Mouvement apparu en 2007, le *quantified self* vise au « mieux-être » par l'analyse de différentes activités liées au mode de vie : un capteur synchronisé avec une application mobile, où sont déclarés certains évènements, mesure les constantes physiques observées lors de ceux-ci. Il s'agit de quantifier une activité ou un paramètre physique (*Runkeeper*, *Runtastic*, *Nike+*, *Fitbit*) ; de surveiller la

nutrition au travers de l'estimation des calories (*MyFitness Pal*) ; de surveiller le poids (balance connectée) ; de suivre un facteur de risque ; de mesurer la qualité du sommeil (*Jawbone*, isommeil,…) etc. Au début de l'été 2012, on recensait ainsi 13 700 applications de santé mobile pour *iOS*, *Android* et *WindowsPhone*, soit 3 % des logiciels dédiés aux *smartphones* et tablettes.

Cependant, en l'absence de réglementation spécifique, on peut se demander quel cadre juridique leur est applicable. On peut estimer que ces logiciels de santé mobile entrent dans les catégories de logiciels de santé d'ores et déjà réglementés, tels que les dispositifs médicaux et les logiciels d'aide à la prescription et à la délivrance des médicaments. Mais les normes qui ont ainsi vocation à s'appliquer à la *m-Health* ne sont que rarement respectées, les développeurs préférant présenter leurs applications comme des « gadgets » ne remplaçant ni un avis médical, ni un produit de santé, et se refusant à garantir l'exactitude des résultats. Quant aux applications de santé mobile « connectées », elles doivent respecter la loi « Informatique et libertés » et les dispositions spécifiques du code de la santé sur la santé numérique, notamment celles relatives à l'hébergement de données. Cependant, de nombreuses données traitées ne relèvent pas à l'évidence de la catégorie des données de santé et ne bénéficient pas de la protection particulière qui s'y attache. Ce cadre juridique est donc peu adapté à des applications qui échappent à toute catégorisation juridique connue. Dès lors, il est parfois préconisé d'instituer une obligation de certification préalable des applications de santé mobile[29]. Dans ce domaine où les frontières entre bien-être et santé sont de plus en plus floues, la problématique du partage des données, notamment avec des tiers, renouvelle la question du respect de la vie privée et de la protection que lui doivent les pouvoirs publics[30].

29. P. Desmarais, « Quel régime pour la m-Health ? », *Communication Commerce électronique*, n° 3, Mars 2013, étude 5.

30. CNIL, « Le quantified self : nouvelle forme de partage des données personnelles, nouveaux enjeux ? » *La lettre Innovation & Prospective*, n°5, juillet 2013 ; CNIL, « Le corps, nouvel objet connecté », *Cahiers Innovation et Prospective*, n°2, mai 2014.

Annexe 4 – Numérique et éducation

Personne ne contestera que l'éducation est elle aussi exposée aux bouleversements liés à la généralisation d'internet et des technologies numériques, qui abolissent les distances et permettent l'accès au savoir où que l'on se trouve. Encore faut-il savoir dans quelle mesure et au prix de quels risques ces technologies peuvent, par les puissants moyens qu'elles offrent, servir le droit fondamental à l'éducation.

L'éducation est un droit fondamental consacré par l'alinéa 13 du Préambule de la Constitution de 1946[31] et, au niveau européen, par la Charte sociale européenne du Conseil de l'Europe, révisée en 1996, en son article 17 alinéa 2[32].

Au niveau international, le Pacte relatif aux droits économiques, sociaux et culturels de 1966[33] et la Convention internationale des droits de l'enfant (CIDE)[34] établissent également ce droit fondamental à l'éducation. Il peut, au même titre que d'autres droits fondamentaux traités dans le cadre de la présente étude du Conseil d'État, tirer profit du numérique : si l'éducation doit être accessible au plus grand nombre sur l'ensemble du territoire, le numérique doit pouvoir, dès lors, grâce à la puissance de ses moyens, participer à l'exercice du droit à l'éducation. Se trouve ainsi pleinement légitimée la mise en place d'un « service public du numérique éducatif ». L'outil informatique, en ce qu'il transcende les distances, peut donner une effectivité nouvelle à l'idéal d'un droit universel à l'éducation.

Le numérique, dans sa dimension du traitement informatique, peut également grandement faciliter l'administration du système éducatif caractérisé, depuis les années soixante, par une forte « massification » en matière d'accueil des élèves. Le traitement des données personnelles permis par la généralisation des outils informatiques favorise l'efficacité du système mais nécessite une vigilance particulière de la part des pouvoirs publics comme des usagers du service public d'éducation. De plus, les enjeux de la protection des données personnelles ne concernent pas seulement les élèves et leurs familles, mais également les enseignants.

31. « *La Nation garantit l'égal accès de l'enfant et de l'adulte à l'instruction, à la formation professionnelle et à la culture. L'organisation de l'enseignement public gratuit et laïque à tous les degrés est un devoir de l'État* ».

32. « *En vue d'assurer aux enfants et aux adolescents l'exercice effectif du droit de grandir dans un milieu favorable à l'épanouissement de leur personnalité et au développement de leurs aptitudes physiques et mentales, les Parties s'engagent à prendre, soit directement, soit en coopération avec les organisations publiques ou privées, toutes les mesures nécessaires et appropriées tendant […] 2. à assurer aux enfants et aux adolescents un enseignement primaire et secondaire gratuit, ainsi qu'à favoriser la régularité de la fréquentation scolaire* ».

33. Article 13, 1er al. : « *Les États parties au présent Pacte reconnaissent le droit de toute personne à l'éducation. Ils conviennent que l'éducation doit viser au plein épanouissement de la personnalité humaine et du sens de sa dignité et renforcer le respect des droits de l'homme et des libertés fondamentales* ».

34. Article 28 : « *Les États parties reconnaissent le droit de l'enfant à l'éducation* », « *rendent l'enseignement primaire obligatoire et gratuit », « encouragent l'organisation de différentes formes d'enseignement secondaire (…) accessible à tout enfant »* et « *assurent à tous l'accès à l'enseignement supérieur, en fonction des capacités de chacun* ».

L'acte d'enseigner étant fondé sur la diffusion du savoir et la duplication des contenus, la mise en place progressive du service public du numérique éducatif oblige, par ailleurs, à une réflexion d'ampleur sur une refonte du droit d'auteur. La loi du 1er août 2006 relative au droit d'auteur et aux droits voisins dans la société de l'information, dite loi « DAVDSI », ou les accords 2012-2013 conclus le 1er février 2012 entre le Centre français d'exploitation du droit de copie (CFC) et le ministère de l'Éducation nationale, de l'Enseignement supérieur et de la Recherche ainsi que la conférence des présidents d'université, permettent déjà une prise en compte de l'outil numérique dans l'enseignement. Mais la mobilisation de nouveaux outils juridiques est, sans doute, plus que jamais nécessaire.

I- Le numérique au service du droit à l'éducation

A. Le « service public du numérique éducatif »

La France n'a pris conscience que récemment de la nécessité d'accélérer le passage à l'école du numérique, à la suite du rapport sur « La structuration de la filière du numérique éducatif : un enjeu pédagogique et industriel »[35], qui a relevé la position médiocre de la France en matière d'« éducation numérique » : selon le dernier cycle d'études du programme international pour le suivi des acquis des élèves, dit « PISA »[36] de 2009, la France n'était à cette date qu'en dixième position sur un ensemble de 16 pays de l'OCDE étudiés, s'agissant du niveau de compréhension de l'écrit électronique par les élèves.

C'est dans ce contexte qu'a été créé un « service public du numérique éducatif » ayant pour mission, grâce à un fort investissement financier et conceptuel, de favoriser une meilleure démocratisation de l'enseignement, et ce faisant, de renforcer la croissance et l'emploi qui sont, au-delà des phénomènes conjoncturels, fortement corrélés au niveau d'éducation de la population.

La loi du 8 juillet 2013 pour la refondation de l'école de la République[37] prévoit dans son article 16 qui réécrit l'article L. 131-2 du Code de l'éducation, que:

« *L'instruction obligatoire peut être donnée soit dans les établissements ou écoles publics ou privés, soit dans les familles par les parents, ou l'un d'entre eux, ou toute personne de leur choix.*

Dans le cadre du service public de l'enseignement et afin de contribuer à ses missions, un service public du numérique éducatif et de l'enseignement à distance est organisé pour, notamment :

1° Mettre à disposition des écoles et des établissements scolaires une offre diversifiée de services numériques permettant de prolonger l'offre des enseignements qui y sont dispensés, d'enrichir les modalités d'enseignement et de faciliter la mise en œuvre d'une aide personnalisée à tous les élèves ;

35. Ministères de l'éducation nationale, de l'enseignement supérieur et de la recherche, de l'économie et des finances, et du redressement productif, « La structuration de la filière du numérique éducatif : un enjeu pédagogique et industriel », Rapport remis en juillet 2013.

36. Acronyme pour « *Program for International Student Assessment* ».

37. Loi n° 2013-595 du 8 juillet 2013 d'orientation et de programmation pour la refondation de l'école de la République.

2° Proposer aux enseignants une offre diversifiée de ressources pédagogiques, des contenus et des services contribuant à leur formation ainsi que des outils de suivi de leurs élèves et de communication avec les familles ;

3° Assurer l'instruction des enfants qui ne peuvent être scolarisés dans une école ou dans un établissement scolaire, notamment ceux à besoins éducatifs particuliers. Des supports numériques adaptés peuvent être fournis en fonction des besoins spécifiques de l'élève ;

4° Contribuer au développement de projets innovants et à des expérimentations pédagogiques favorisant les usages du numérique à l'école et la coopération.

Dans le cadre de ce service public, la détermination du choix des ressources utilisées tient compte de l'offre de logiciels libres et de documents au format ouvert, si elle existe. »

La création d'une direction numérique de l'éducation (DNE) par le décret du 18 février 2014[38] traduit ce choix dans l'organigramme du ministère de l'Education nationale. L'organisation de la DNE en deux services illustre les différents enjeux du numérique dans l'éducation : l'aspect pédagogique est pris en charge par un « service du développement du numérique éducatif » tandis que la sécurisation des procédures et des outils mis au service du numérique éducatif relève du « service des technologies et des systèmes d'information ».

Si cette évolution du service public de l'éducation apporte une illustration du principe de mutabilité ou d'adaptabilité du service public, elle ne garantit pas, par elle-même, l'atteinte des résultats. Comme le remarquent Pierre-Laurent Frier et Jacques Petit, « *L'éducation nationale faillirait à sa mission si elle n'évoluait pas pour tenir compte de la révolution informatique, mais le nombre d'ordinateurs à implanter dans les établissements scolaires ne lui est pas fixé par le droit !* »[39].

B. Les MOOCs dans l'éducation : vers une université numérique ?

Le développement récent des « *Massive Open Online Courses* » (MOOCs), appelés également « FLOTS» (Formations en ligne ouvertes à tous) ou « CLOMS » (cours en ligne ouverts et massifs) par les universités françaises, illustre les potentialités du numérique dans le domaine de l'éducation. Les MOOCs, puisque c'est cet acronyme que l'on propose de retenir, permettent en effet à un grand nombre de personnes, qui ne sont pas tous des étudiants, de se former à distance en suivant des enseignements disponibles en ligne. Ils combinent divers outils : texte, images, vidéo, « *podcasts* », etc.

Dans le rapport de la mission parlementaire « Apprendre autrement à l'ère numérique »[40], le député Jean-Michel Fourgous inventorie les différents outils

38. Décret n° 2014-133 du 17 février 2014 fixant l'organisation de l'administration centrale des ministères de l'éducation nationale et de l'enseignement supérieur et de la recherche, publié au JORF n° 0041 du 18 février 2014.

39. P.-L. FRIER, J. PETIT, *Droit administratif*, Paris, Montchrestien, Lextenso éditions, 2012.

40. *Apprendre autrement à l'ère numérique. Se former, collaborer, innover : Un nouveau modèle éducatif pour une égalité des chances*, Rapport de la mission parlementaire de Jean-Michel Fourgous, député des Yvelines, sur l'innovation des pratiques pédagogiques par le numérique et la formation des enseignants,

numériques pouvant être mobilisés utilement au service de l'éducation. Ainsi par exemple, l'« *e-learning* » pourrait être mobilisé en tant que « *support de l'égalité des chances* »[41] et combattre les effets des inégalités sociales, en limitant les redoublements de classe dont l'efficacité est souvent contestable. Le rapport parlementaire propose également de développer le potentiel interactif des « *environnements numériques de travail* » qui, comme les techniques de « *e-learning »*, favorisent la continuité des apprentissages.

Cependant les MOOCs sont porteurs d'une nouveauté plus radicale, car à la différence des techniques dites de « *e-learning* », qui servent surtout à « appuyer » certains cours, le MOOC pourrait avoir vocation à se substituer à l'enseignement physique. Source potentielle de préoccupations chez certains enseignants[42], le MOOC est surtout facteur d'innovation : il serait démocratique par sa nature même, puisque gratuit et ouvert à tous sans aucune condition susceptible d'instaurer une discrimination dommageable à certains étudiants. Les MOOCs qui sont à l'heure actuelle diffusés massivement dans certains pays en développement offrent, de plus, une réelle opportunité aux élèves dont le désir d'apprendre est souvent entravé par l'inadaptation des structures universitaires. Leur gratuité est également un atout important, non seulement aux États-Unis où la plupart des formations universitaires reconnues sont très onéreuses, mais également en France, puisque l'État doit assurer des coûts non apparents mais analogues.[43]

Pour autant, les MOOCs présentent des biais non négligeables quoique souvent sous-estimés. Ils portent principalement sur la certification de la qualité des cours, l'évaluation des connaissances acquises, les nombreuses possibilités de fraude, difficiles à juguler. À cela s'ajoute le fait que les MOOCs seraient porteurs de discrètes mais réelles discriminations, en ce qu'ils seraient, notamment, adaptés aux élèves les plus autonomes.

Les MOOCs n'échappent pas par ailleurs au modèle économique du *net*, illustré par le succès des plateformes de formation ouverte et de masse telles que *Coursera* ou *Udacity*, créées en marge de l'université californienne de Stanford. En effet, à côté des cours gratuits, les plateformes proposent des certifications payantes ou des services annexes rémunérés, tels que ceux liés à la mise en relation avec des employeurs.

Remis le 24 février 2012, 237 pages: http://www.education.gouv.fr/archives/2012/refondonslecole/wpcontent/uploads/2012/07/rapport_fourgous_apprendre_autrement_a_l_ere_numerique_fevrier_2012.pdf

41. *Ibid*., p. 162.

42. Ph. BERNARD, « Les MOOCs, nouvelle frontière de l'Université », Article du 3 avril 2014 publié sur Le Monde et accessible via ce lien : http://abonnes.lemonde.fr/enseignement-superieur/article/2014/04/03/les-moocs-nouvelle-frontiere-de-l-universite_4395542_1473692.html?xtmc=universite_2_0&xtcr=2

43. P. ENGEL, « Les MOOCS : Cours massifs ou armes de destruction massive ? », Tribune du 24 mai 2013 du site Qualité de la Science française, consultable sur http://www.qsf.fr/2013/05/24/les-moocs-cours-massifs-ou-armes-de-destruction-massive-par-pascal-engel/

De manière plus générale, l'éducation est désormais appelée à entretenir une relation privilégiée avec le *Big Data* : parmi les avantages escomptés, figure le potentiel de personnalisation présenté par les MOOCs. Des *start-ups* d'éducation en ligne développent ainsi des algorithmes qui recueillent massivement les données émises par les élèves au cours de la journée. Ces données répertorient aussi bien le pourcentage d'erreurs relevées dans des situations typiques dûment analysées que les habitudes comportementales d'apprentissage en fonction des heures d'une journée. Ces analyses permettent à la plateforme de mettre en place des technologies d'apprentissage adaptées (*adaptative learning*) dont le but ultime est d'obtenir un étalonnage des taux de réussite les plus probants. L'objectif des MOOCs n'est donc pas seulement la diffusion la plus large possible d'enseignements, il s'agit également, en arrière plan, de mieux cerner les habitudes d'apprentissage des internautes[44] : c'est ainsi que le *Big Data* rejoint l'éducation ou que l'éducation est, si l'on peut dire, « rattrapée », par le *Big Data*.

Les plateformes d'enseignement en ligne posent enfin la question du rôle que jouent les pouvoirs publics en matière d'éducation. Le « *e-learning* », fréquemment utilisé par les universités elles-mêmes, apparaissait comme une extension, un complément des enseignements « physiques » traditionnels. Au contraire, les MOOCs en rapide croissance ainsi que de nombreuses plateformes commerciales d'enseignement font bien souvent figures de concurrents à l'enseignement dispensé dans le cadre du service public de l'éducation. Dès lors qu'elles prétendent répondre aux besoins des élèves autrement que ne le font les structures classiques d'enseignement, on peut se demander si ces plateformes ne se constituent pas en modes alternatifs d'enseignement et d'apprentissage, pour contester la position des personnes publiques chargées des différents niveaux d'enseignement.

Ces interrogations sont renforcées par la remise en cause, par certaines plateformes numériques, du principe du diplôme comme sanction d'un niveau donné de connaissances et de capacités. On a pu se demander si « *la question de la valeur des diplômes à long terme pourrait se poser* »[45]. Est donné notamment l'exemple de « l'école d'informatique 42 », fondée par le dirigeant du groupe de télécommunication *Illiad* et du fournisseur d'accès *Free*, Xavier Niel, qui ne propose pas, à l'issue des formations dispensées, de diplômes, mais des « badges » délivrés au terme de modules d'enseignement suivis intégralement et évalués.

D'autres arguments vont dans le sens d'un rôle renouvelé de l'État. Certains projets de plateformes d'enseignement ont été mis en place directement par les pouvoirs publics, comme « France Université Numérique » (FUN) créée à l'automne 2013 par le ministère de l'enseignement supérieur et de la recherche[46]. La mise en place d'un MOOC nécessite des investissements importants. Le coût de la création d'un

44. J.-M. GILLIOT, « Moi je mooc, et vous ? », Article publié le 28 avril 2014 sur le Blog du monde *Binaire. L'informatique : la science au cœur du numérique*, consultable sur Le Monde.fr édition abonnés à http://binaire.blog.lemonde.fr/2014/04/28/moi-je-mooc-et-vous/.

45. G. BABINET, « Avec les MOOCs, préparez-vous à passer des diplômes aux badges. », Tribune du Cercle Les Echos.fr, « Éducation », Rubrique « Économie et société », 15/11/2013, consultable sur : http://lecercle.lesechos.fr/economie-societe/societe/education/221184388/moocs-preparez-a-passer-diplomes-aux-badges.

46. Voir le site consacré à la plateforme FUN : http://www.france-universite-numerique.fr/18-actions.html.

module est de l'ordre de 50 000 euros.[47] Si les grandes universités ont généralement les moyens de s'offrir une « extension en ligne » de leurs cours et de recruter des professeurs susceptibles de fidéliser un auditoire, les universités plus modestes sont rarement en mesure de créer un MOOC de renommée internationale ou même nationale. Les pouvoirs publics peuvent toutefois remédier à cette inégalité en offrant un soutien en termes d'organisation et de moyens financiers.

Les MOOCs sont donc incontestablement porteurs d'innovations pédagogiques, y compris en faveurs des étudiants présents sur le campus. Mais la révolution annoncée ne sera accomplie que sous réserve d'une évaluation rigoureuse, méthodique et continue de ce qu'ils apprennent réellement aux étudiants.

II. Les enjeux de la protection des données personnelles pour les élèves et les enseignants

A. Les fichiers d'élèves

En juillet 2010, le Conseil d'État a eu à juger de la légalité de deux fichiers de l'éducation nationale, dénommés « BE1D » (Base élèves premier degré) et « BNIE » (Base nationale des identifiants élèves). Ces fichiers permettent le suivi administratif et pédagogique des élèves des écoles maternelles et primaires. Les contentieux liés à ces fichiers posaient la question de leur conformité à la loi dite « informatique et libertés » du 6 janvier 1978.

S'agissant du fichier BE1D, le Conseil d'État a en particulier censuré la collecte telle qu'elle ressortait de la première version du fichier de données relatives à l'affectation des élèves en classe d'insertion scolaire (CLIS)[48]. Ces informations étaient en effet d'une précision telle qu'il était possible d'avoir connaissance du handicap d'un certain nombre d'élèves. Les données du fichier présentaient, pour certaines d'entre elles, le caractère de données de santé. La censure portait également sur des dispositions du fichier qui rendaient impossible, au regard de l'article 38 de la loi de 1978, l'exercice du droit d'opposition.

Concernant le fichier BNIE[49], le Conseil d'État a souligné l'importance, au regard de la loi de 1978, du respect par l'administration du principe de proportionnalité : il a jugé que ce fichier était irrégulier en ce que la durée prévue de conservation des données était de 35 ans, alors que le ministère ne justifiait pas suffisamment une telle durée de conservation au regard des finalités de traitement.

Ces décisions du Conseil d'État mettent en lumière l'ambivalence de l'outil numérique. Celui-ci permet de disposer d'informations utiles à la connaissance pédagogique des élèves, au suivi statistique de cohortes de jeunes scolarisés et au pilotage du système éducatif lui-même. En revanche, le juge rappelle que cette collecte doit strictement correspondre aux finalités du traitement et ne pas empiéter sur des libertés fondamentales.

47. N. SILBERT, « L'enseignement français face au défi des cours en ligne », Article en ligne sur LesEchos.fr, consultable via ce lien : http://www.m.lesechos.fr/redirect_article.php?id=0203377463800.

48. CE, 19 juillet 2010, *M. F… et Mme C…*, n° 317182 et 323441, Rec. p. 320.

49. CE, 19 juillet 2010, *M. F… et Mme C…*, n° 334014, Rec. pp. 777, 779 et 916.

B. L'évaluation et la notation des enseignants sur internet

L'usage des technologies numériques a également soulevé de délicates questions portant sur l'évaluation et la notation des professeurs sur internet. Dans une ordonnance de référé du 3 mars 2008[50], le tribunal de grande instance de Paris s'est prononcé sur la légalité du site internet « *note2be* ». Celui-ci permettait aux élèves internautes de noter les enseignants répertoriés sur le site, de rechercher les noms de professeurs au moyen d'une barre de recherche apparaissant en tête du site, afin de les noter mais aussi de prendre connaissance des différentes notes attribuées par d'autres internautes. Le site renvoyait par ailleurs à un forum, lequel contenait des encadrés reprenant les derniers sujets discutés et répartissant les professeurs en plusieurs catégories, notamment un « *top 10* » mais également une rubrique « *sales profs…* ». Les demandeurs soutenaient que le site était générateur d'un « *trouble manifestement illicite* » auquel il convenait de mettre un terme. Ils soulignaient notamment que la collecte et l'utilisation de données nominatives afin d'effectuer des évaluations individuelles n'étaient autorisées par aucune disposition de la loi « informatique et libertés » de 1978.

Le juge des référés a examiné l'affaire après avoir écarté les moyens tenant à la vie privée au sens de l'article 9 du code civil, en relevant qu'il s'agissait d'une évaluation de l'activité professionnelle d'enseignants sur Internet. La possibilité pour les élèves d'évaluer et de noter des enseignants sur le site relève quant à elle de la liberté d'expression. En se fondant sur l'article 7, 5° de la loi de 1978, le juge des référés établit que la SARL *Note2be.com* ne peut défendre son site qu'en prouvant qu'il contribue à « *la réalisation de l'intérêt légitime poursuivi par le responsable du traitement ou par le destinataire, sous réserve de ne pas méconnaître l'intérêt ou les droits et libertés fondamentaux de la personne concernée* »[51]. C'est cette méconnaissance de l'intérêt ou des droits et libertés fondamentaux de la personne concernée qui est apparue caractérisée aux yeux du juge. Celui-ci relève ainsi que les différents qualificatifs proposés dans la notation des enseignants orientent l'évaluation des élèves internautes, alors que le point de vue des enseignants n'est pas pris en compte ; l'équilibre entre les intérêts du responsable de traitement et les droits des personnes concernées que requiert le 5° de l'article 7 de la loi du 6 janvier 1978 n'était donc pas assuré. Pour cette raison, le juge des référés a condamné la société à « *suspendre sur le site www.note2be.com l'utilisation de données nominatives d'enseignants aux fins de leur notation et leur traitement, ainsi que leur affichage sur les pages du site en question* ».

Par un arrêt du 25 juin 2008[52], la cour d'appel de Paris a confirmé l'ordonnance du juge des référés en estimant que le site représentait un « *trouble manifestement illicite* » dès lors que tous les élèves pouvaient noter les professeurs, quand bien même ils n'avaient pas eu le professeur comme enseignant et que les données du site n'avaient pas été collectées « *de façon loyale* ».

---

50. Tribunal de grande instance de Paris, 3 mars 2008, ordonnance n° 08-51650.

51. Article 7, 5° de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, modifié par la loi n°2004-801 du 6 août 2004, art. 2, JO du 7 août 2004.

52. Cour d'appel de Paris, 14ème chambre, sanction A, 25 juin 2008.

III. La question des droits d'auteur dans l'emploi des ressources éducatives numériques.

A. Le cadre juridique actuel : les possibilités restreintes d'usage du numérique dans l'éducation

Dès lors que le système éducatif était appelé à évoluer en réponse à la révolution numérique, il a paru nécessaire de faciliter l'utilisation par les enseignants d'œuvres sur support numérique. Ce fut l'objet de la loi DADVSI[53] qui, outre des mesures de lutte contre le piratage, contient des dispositions d'adaptation des droits d'auteur aux usages numériques. La loi assure la transposition en droit interne de la directive 2001/29/CE du Parlement européen et du Conseil du 22 mai 2001 sur l'harmonisation de certains aspects du droit d'auteur et des droits voisins dans la société de l'information. Ainsi, le code de la propriété intellectuelle prévoit en son article L. 122-5 des exceptions au droit d'auteur permettant la représentation ou la reproduction d'extraits d'œuvres dans un cadre pédagogique, l'article précisant notamment la composition du public pouvant bénéficier de l'exception[54]. Enfin, cette exception pédagogique ne vaut que « *sous réserve d'une rémunération négociée sur une base forfaitaire* » et ne soustrait donc pas le secteur éducatif aux règles du droit d'auteur.

Cette négociation a eu lieu dans le cadre d'accords sectoriels entre les ministères et les sociétés de gestion collective représentants les auteurs. Les règles varient désormais selon les œuvres et selon le type d'usage qui en est fait. Elles distinguent les livres selon qu'ils sont « œuvres conçues à des fins pédagogiques » (OCFP) ou non, les publications périodiques, la musique imprimée ou encore les œuvres des arts visuels, issues ou non d'une publication. S'agissant des usages des œuvres, les régimes sont différents selon que l'on se situe dans le cadre pédagogique de la classe ou selon qu'il s'agit de sujets d'examens ou de cours mis en ligne sur le site des établissements.

---

53. Loi n° 2006-961 du 1er août 2006 relative au droit d'auteur et aux droits voisins dans la société de l'information, JO du 3 août 2006.

54. Article L. 122-5 modifié par la loi n° 2011-1898 du 20 décembre 2011, art. 1 : « *Lorsque l'œuvre a été divulguée, l'auteur ne peut interdire (…) 3° Sous réserve que soient indiqués clairement le nom de l'auteur et la source », « e) La représentation ou la reproduction d'extraits d'oeuvres, sous réserve des oeuvres conçues à des fins pédagogiques, des partitions de musique et des oeuvres réalisées pour une édition numérique de l'écrit, à des fins exclusives d'illustration dans le cadre de l'enseignement et de la recherche, à l'exclusion de toute activité ludique ou récréative, dès lors que le public auquel cette représentation ou cette reproduction est destinée est composé majoritairement d'élèves, d'étudiants, d'enseignants ou de chercheurs directement concernés, que l'utilisation de cette représentation ou cette reproduction ne donne lieu à aucune exploitation commerciale et qu'elle est compensée par une rémunération négociée sur une base forfaitaire sans préjudice de la cession du droit de reproduction par reprographie mentionnée à l'article L. 122-10.* »

B. Des solutions pour faire pleinement bénéficier l'éducation des possibilités ouvertes par le numérique

Soulignée par de nombreux observateurs, la complexité de ces règles fait obstacle à l'utilisation du numérique par les enseignants. Plusieurs pistes d'évolution sont avancées dans le débat public.

Le rapport « Apprendre autrement à l'ère numérique » de Jean-Michel Fourgous, évoqué ci-dessus, appelle par exemple de ses vœux une nouvelle réforme, l'adaptation des droits d'auteur au numérique par la loi DAVDSI n'étant pas selon lui satisfaisante, en raison des concessions faites dans les accords sectoriels. Le rapport évoque les licences *Creatives Commons*, qui reposent sur « *une organisation à but non lucratif qui facilite le partage et la réutilisation de la créativité et de la connaissance à travers des outils juridiques gratuits »* et qui sont proposées comme une alternative crédible aux droits d'auteur, présentant l'avantage de faciliter l'utilisation d'œuvres dans un contexte éducatif et donc de profiter de l'immense potentiel que présente internet en matière d'éducation. Dans ce système, les titulaires de droits seraient en mesure de définir les conditions dans lesquelles ils souhaitent voir leur œuvre utilisée et les utilisateurs ne seraient pas dans l'obligation de négocier périodiquement des autorisations avant de pouvoir utiliser l'œuvre en question. Il s'agirait ainsi de privilégier le recours à l'« *Open Source* » dans le domaine pédagogique. Des projets permettant de mettre en ligne, gratuitement, des contenus pédagogiques (« *Open Course Ware* ») à l'image de ce que propose la plateforme « France Université Numérique » (FUN), déjà évoquée ci-dessus, pourraient être mis en place en utilisant un grand nombre de licences ouvertes ou peu contraignantes.

*
**

En conclusion de cette annexe, il est permis de relever que nombre des grands enjeux juridiques du numérique sont présents dans la sphère si particulière de l'éducation. Les exemples qui viennent d'être traités l'attestent, qu'il s'agisse des garanties à protéger pour l'utilisation des données personnelles, des précautions à prendre en vue d'un service loyal attendu des plateformes de formation en ligne ouvertes à tous ou encore de la juste modulation des droits d'auteurs pour tenir compte du support numérique des créations utilisées à des fins éducatives.

Annexe 5 – Numérique et relations du travail

La présence croissante du numérique dans les relations du travail a des incidences sur les droits et libertés fondamentaux qui régissent celles-ci, notamment :
- le droit au respect de la vie privée des travailleurs ;
- le droit au repos, garanti par le onzième alinéa du Préambule de la Constitution de 1946 ;
- la liberté d'expression des salariés dans et en dehors du travail ;
- la liberté syndicale ;
- le droit à l'emploi, proclamé par le cinquième alinéa du Préambule de 1946.

I. Le droit à la protection de la vie privée du salarié et les pouvoirs de surveillance de l'employeur

Le numérique, *via* le développement des technologies de l'information et de la communication, rend plus facile l'irruption de la vie privée du salarié au sein de la sphère du travail. L'employeur voit se renforcer potentiellement son pouvoir de surveillance du salarié dans l'exécution de son travail. La loi et la jurisprudence ont évolué pour trouver un équilibre entre le respect des droits fondamentaux du salarié et la reconnaissance de possibilités de contrôle par l'employeur.

A. La définition de la vie privée en matière de droit du travail

En matière de droit du travail, l'article L. 1121-1 du Code du travail dispose que « *nul ne peut apporter aux droits des personnes et aux libertés individuelles et collectives des restrictions qui ne seraient pas justifiées par la nature de la tâche à accomplir, ni proportionnées au but recherché* ». Dans son arrêt *Niemietz* du 16 décembre 1992 (n° 13710/88), la CEDH a affirmé « *qu'il serait trop restrictif de limiter la vie privée à un cercle intime où chacun peut mener sa vie personnelle à sa guise et d'en écarter entièrement le monde extérieur à ce cercle* » et qu'« *il n'y a aucune raison de principe d'en exclure les activités professionnelles ou commerciales* ».

En France, la décision juridictionnelle de principe en matière du respect de la vie privée des travailleurs est l'arrêt de la Cour de cassation *Nikon* du 2 octobre 2001, qui adopte une position voisine de celle de la CEDH. Le salarié a droit au respect de l'intimité de sa vie privée, « *même au temps et au lieu de travail* ». Ainsi l'employeur, bien qu'étant en droit d'exercer un certain contrôle justifié sur l'activité de ses employés, ne peut pas prétendre utiliser n'importe quel moyen.

1. Les limites au pouvoir de surveillance de l'employeur

L'employeur s'attend raisonnablement à ce que l'employé se consacre à son travail lorsqu'il est sur son lieu et dans son temps de travail. De là découle son pouvoir de surveillance : « *l'employeur a le droit de contrôler et de surveiller l'activité de ses salariés pendant le temps de travail* », « *seul l'emploi de procédés clandestins*

est illicite »[55]. Comme la chambre sociale, la chambre criminelle de la Cour de cassation a reconnu dans son arrêt *Nortel* du 19 mai 2004[56] que l'employeur a un pouvoir de contrôle et de surveillance de l'activité du salarié. Il peut ainsi appliquer son pouvoir de sanction le cas échéant.

Toutefois ce pouvoir est susceptible d'abus, notamment via le recours à la technologie : les possibilités sont nombreuses, de la vidéosurveillance aux dispositifs biométriques. Au fur et à mesure de l'arrivée des nouvelles technologies dans le monde du travail, la jurisprudence a fixé des limites au pouvoir de contrôle de l'employeur.

a) Les outils de travail informatique mis à disposition du travailleur

Les outils de travail informatique mis à disposition du travailleur, tels que l'ordinateur connecté à internet et la messagerie interne, sont d'usage courant sur les lieux de travail. Une utilisation personnelle est tolérée par les tribunaux, si elle reste raisonnable et n'a pas de répercussions particulières sur le travail.

Dès lors, l'employeur peut contrôler et limiter l'usage d'internet et de la messagerie. Le principe en la matière est que le contenu de la messagerie étant présumé avoir un caractère professionnel, l'employeur peut lire son contenu en dehors de la présence du salarié, sauf si le caractère personnel est explicitement affiché. Le même principe s'applique aux fichiers contenus dans l'ordinateur. Le juge considère que *« dès lors que la formulation utilisée confère au courrier ou au fichier un caractère privé, même s'il n'est pas formellement identifié comme personnel, l'employeur ne devrait pas être autorisé à l'ouvrir en dehors de la présence du salarié »*[57]. Cette protection peut être levée en cas d'enquête judiciaire ou d'autorisation explicite du juge : l'employeur peut ainsi demander d'accéder aux dossiers et messages personnels, en présence d'un huissier. Cependant si des fichiers non référencés comme personnels sont ouverts et s'avèrent être d'ordre privé, ils ne peuvent être utilisés pour sanctionner le salarié[58]. La CNIL recommande dans sa fiche pratique ***« Le contrôle de l'utilisation d'internet et de la messagerie »***[59] d'informer les salariés sur le principe retenu pour différencier les e-mails professionnels des e-mails personnels, par exemple en l'intégrant dans une charte.

Quant aux clés USB, une clé sans dénomination particulière connectée à un outil professionnel est présumée avoir un caractère professionnel : l'employeur peut y avoir accès hors la présence du salarié, d'après l'arrêt dit *Clé USB* du 12 février 2013[60]. Si la clé est présumée personnelle, en raison de son apparence par exemple, l'employeur peut la retirer de l'ordinateur, sanctionner le salarié en application du règlement intérieur et prendre connaissance de son contenu en présence du salarié ou si ce dernier a été dûment appelé.

55. Cass. Soc., 20 novembre 1991.

56. Cass., Crim., 19 mai 2004, *Jean-Francois L. c/ société Nortel networks*.

57. B. Bossu « Ouverture d'un courriel par l'employeur et utilisation de son contenu », *La Semaine Juridique Social* n° 5**,** 31 Janvier 2012, 1041.

58. Cass., Soc., 5 juillet 2011, *Sté Gans Assurances IARD*.

59. Disponible sur le site www.cnil.fr.

60. Cass., Soc., 12 février 2013, n° 11-28.649, Bull. 513.

b) Les dispositifs de surveillance

En cas de mise en place d'un dispositif de surveillance, celui-ci doit être au préalable porté à la connaissance du salarié[61] et faire l'objet d'une information et d'une consultation du comité d'entreprise[62]. Les fichiers et traitements automatisés doivent faire l'objet d'une déclaration à la CNIL[63].

Les dispositifs biométriques doivent être autorisés par la CNIL. La doctrine élaborée par la CNIL prend en compte les éléments suivants : la limitation des finalités, la proportionnalité du système aux finalités (notamment par la limitation à une zone déterminée représentant un enjeu majeur dépassant les seuls intérêts de l'entreprise), la limitation du nombre de personnes accédant aux données, la sécurisation du système.

La géolocalisation des véhicules d'entreprise se développe également. Ici encore les instances représentatives du personnel doivent être informées et consultées avant la mise en place du dispositif, qui doit faire l'objet d'une déclaration à la CNIL, sauf si l'entreprise comprend un CIL (c'est lui qui devra noter la mise en place du dispositif dans son registre). Selon une recommandation de la CNIL du 16 mars 2006, les données collectées ne doivent pas être conservées plus de deux mois[64].

II. Le droit au repos et le temps de travail à l'épreuve du numérique

Le numérique a d'abord facilité le développement d'une nouvelle organisation du travail, le télétravail (A). Dans un monde de plus en plus dématérialisé, la frontière entre temps de travail et temps de repos devient de plus en plus poreuse ; l'enjeu devient alors le droit à la déconnexion (B).

A. Le régime juridique du télétravail

C'est dans les années 1990 que les pouvoirs publics commencent à s'intéresser à cette forme de travail[65]. En 2002, les partenaires sociaux européens signent un accord-cadre interprofessionnel sur le télétravail. L'accord national interprofessionnel (ANI) français du 19 juin 2005 transpose l'accord européen en droit interne. Le télétravail y est défini comme « *une forme d'organisation et/ou de réalisation du travail, utilisant des technologies de l'information dans le cadre d'un contrat de travail et dans laquelle un travail, qui aurait également pu être réalisé dans les locaux de l'employeur, est effectué hors de ces locaux de façon régulière* ». Selon cet ANI, le télétravailleur bénéficie des mêmes droits que ceux applicables aux salariés travaillant dans les locaux de l'entreprise. L'article 9 précise que « […]

61. Cass., Soc., 22 mai 1995, et articles L. 1222-4 et L. 121-8 du code du travail.
62. Article L. 2323-32 du code du travail.
63. Article 22 de la loi du 6 janvier 1978 modifiée.
64. Un an si elles sont utilisées pour optimiser l'activité, cinq si elles sont utilisées pour le suivi du temps de travail. Cf. la délibération n° 2006-066 du 16 mars 2006.
65. Rapport Breton de 1993 ; appel à projet de la DATAR (Délégation interministérielle à l'aménagement du territoire et à l'attractivité régionale) : « Le télétravail : outil pour l'emploi et la reconquête des territoires ».

la charge de travail, les normes de production et les critères de résultats exigés doivent être équivalents à ceux des salariés en situation comparable travaillant dans les locaux de l'employeur ».

La loi du 22 mars 2012 a inscrit dans le code du travail[66] certaines des autres garanties prévues par l'ANI, notamment le caractère volontaire du télétravail, sa réversibilité (le salarié peut revenir à une exécution du contrat de travail sans télétravail) et l'obligation pour l'employeur de convenir avec le salarié des plages horaires durant lesquelles il peut le contacter.

Selon un rapport du Centre d'analyse stratégique de 2009, qui combine les résultats de trois enquêtes portant sur quinze pays de l'OCDE, le télétravail reste peu développé en France (5 à 10 % de salariés seraient concernés). Une récente enquête menée auprès de vingt grandes entreprises[67] montre cependant un certain essor, avec un taux estimé à 16,7 % en 2012. Mais si le taux progresse, il continue à se heurter à de fortes oppositions. Ainsi, 78 % des managers d'entreprises doutent de la capacité d'assurer l'efficacité des équipes avec cette forme de travail et 55 % pensent qu'elle est incompatible avec la culture de l'entreprise.

L'Organisation internationale du travail promeut les avantages du télétravail. Elle relève **«** *que les télétravailleurs ont tendance à être plus productifs et même à travailler davantage que leurs homologues exerçant au bureau. Selon la synthèse d'études sur le télétravail, quelques grandes sociétés, notamment Best Buy, British Telecom et Dow Chemical, rapportent que les télétravailleurs sont 35 à 40 % plus productifs* **»**[68]. L'étude relève également que le télétravail réduit l'absentéisme (de 63 % en moyenne) grâce à la flexibilité des horaires. Le télétravail permet également de réduire les coûts immobiliers et énergétiques.

B. Vers un droit à la déconnexion ?

Dès 2002, le droit à la déconnexion était une notion reconnue par le Forum des droits sur Internet, comme le rappelle un rapport du Centre d'analyse stratégique autour de l'impact des technologies des l'information et de la communication (TIC) sur les conditions de travail de 2012[69]. Douze ans plus tard, le droit à la déconnexion ne s'est pourtant pas imposé. Il est en effet devenu normal *pour la plupart des individus* de recevoir une notification sur leur smartphone le dimanche indiquant une réunion pour le lendemain à 8h, mais également de prévoir leurs vacances entre deux réunions. On a assisté ces dernières années à un rapprochement des sphères privées et professionnelles par l'usage croissant des TIC.

La jurisprudence et le dialogue social se sont efforcés d'encadrer cette évolution afin de préserver le droit au repos du salarié. La Cour de cassation a rappelé dans

66. Articles L. 1222-9 à L. 1222-11.
67. http://tourdefranceduteletravail.fr/wp-content/uploads/2013/03/Infographie_TourTT.pdf.
68. OIT, 25 mars 2013, communiqué « L'OIT présente les atouts du travail à domicile », *La Semaine Juridique - Social* n° 14, 2 Avril 2013, act. 164.
69. http://www.strategie.gouv.fr/system/files/raptic_web_light_final28022012.pdf.pdf_0.pdf

un arrêt du 17 février 2004 que le fait de ne pas pouvoir joindre un salarié en dehors des horaires de travail sur son téléphone portable personnel ne constitue pas une faute disciplinaire et ne justifie donc pas un licenciement.

Dans le même sens, les entreprises prennent de nombreuses initiatives en France et à l'étranger. En Belgique, *Total* et *Siemens* envisagent ainsi de laisser leurs salariés choisir s'ils souhaitent répondre à leurs courriels en dehors des heures de bureau. De manière plus radicale, *Volkswagen* en Allemagne a bloqué l'accès des téléphones professionnels de 18h15 à 7h du matin[70]. En France, un accord sur le développement et la qualité de vie au travail au sein d'Areva du 31 mai 2012[71] prévoit la nécessité de veiller à ce que l'usage des TIC respecte la qualité du lien social au sein des équipes et ne devienne pas facteur d'isolement sur le lieu de travail ; un article mentionne explicitement le droit de déconnexion des salariés. La garantie du droit à la déconnexion peut être vue comme un enjeu de productivité pour les entreprises : une expérimentation de Leslie Perlow[72], professeur à la *Harvard Business School*, avait démontré que la moitié de ceux qui se déconnectent avaient, après expérience, hâte de venir travailler le matin, contre 27 % de leurs collègues qui ne le faisaient pas.

Les partenaires sociaux de l'économie numérique ont conclu le 7 avril 2014 un accord de branche remarqué relatif au droit à la déconnexion[73], plus précisément à une *« obligation de déconnexion des outils de communication à distance ».* L'accord concerne 250 000 salariés travaillant au forfait jours.

III. La liberté d'expression individuelle et collective des salariés et la liberté syndicale

La liberté d'expression fait partie, avec le droit au respect de la vie privée, des droits dont l'application est bouleversée par l'arrivée des TIC dans le monde du travail. Si un droit d'expression directe et collective est reconnu aux salariés depuis la loi du 4 août 1982, le numérique élargit de manière considérable les possibilités effectives d'expression. Cela représente un véritable enjeu de *e-réputation* pour les individus en termes de chances de recrutement par exemple, mais également pour les entreprises. Celles-ci doivent ainsi faire face à des atteintes à leur *e-réputation* pouvant provenir de tiers, mais également de leurs propres salariés ou des organisations de représentation des salariés.

Le développement des réseaux sociaux en ligne est relativement récent mais il bouleverse de plus en plus les usages d'internet par les travailleurs. Certes la notion de réseau au sein de l'entreprise n'a pas attendu l'arrivée d'internet pour

70. http://www.lefigaro.fr/flash-eco/2011/12/23/97002-20111223FILWWW00288-treve-de-blackberry-chez-volkswagen.php
71. http://www.areva.com/news/liblocal/docs/CP_groupe/2012/CP%20AREVA%20Accord%20Qualite%20de%20vie%20au%20Travail.pdf
72. http://abonnes.lemonde.fr/idees/article/2012/05/09/se-deconnecter-est-la-meilleure-facon-de-se-parler_1697736_3232.html
73. http://www.lesechos.fr/economie-france/social/0203424438907-syntec-reconnait-le-droit-des-cadres-a-la-deconnexion-662543.php

se développer : les travailleurs ont depuis longtemps l'habitude d'échanger régulièrement autour de la machine à café ou à l'heure du déjeuner. Mais les réseaux sociaux tels que *Facebook* et *LinkedIn* utilisent la technique de la liste « d'amis » et de « connaissances possibles » comme outil de navigation. Autre caractéristique, le contenu de ces réseaux est très majoritairement participatif. Ainsi, les conversations entre collègues qui avaient très peu de chances d'être enregistrées par la machine à café acquièrent à travers les réseaux internet une visibilité pouvant porter tort au salarié ou à l'employeur.

De manière générale, la jurisprudence impose aux travailleurs de s'abstenir de tous propos injurieux et diffamatoires à l'égard de leur employeur. Lorsque des propos de cette nature sont proférés à l'égard de l'entreprise et des employeurs sur un réseau social, l'employeur peut donc être tenté de les sanctionner. La question est alors de déterminer si les réseaux externes à l'entreprise, tels que *Facebook*, *LinkedIn* et *Twitter*, relèvent de la sphère publique ou privée.

Selon la jurisprudence actuellement majoritaire, il convient, au cas par cas, de prendre en compte le degré d'ouverture du compte afin de déterminer si la ou les pages contenant les propos mis en cause peuvent être qualifiées de correspondances privées ou de communications publiques. Ainsi le 19 novembre 2010, le conseil de prud'hommes de Boulogne-Billancourt a considéré que la page *Facebook* sur laquelle étaient inscrits les propos diffamatoires pouvait potentiellement être lue par des personnes extérieures, au vu du mode de paramétrage du compte. Quand le caractère « ouvert » de la page ne peut pas être établi avec certitude, les juges ont tendance à considérer que le licenciement ou la sanction est sans cause réelle et sérieuse[74]. Ainsi les propos tenus sur un compte *Facebook* public ou ouvert « *aux amis d'amis* », peuvent être considérés comme publics. Un arrêt du 10 avril 2013 de la Cour de cassation précise cette jurisprudence en relevant que « *les propos litigieux avaient été diffusés sur les comptes ouverts tant sur le site Facebook que sur le site MSN, lesquels n'étaient en l'espèce accessibles qu'aux seules personnes agréées par l'intéressée, en nombre très restreint* »[75]. Les personnes en question formant une communauté d'intérêts, les propos ne peuvent être qualifiés d'injures publiques.

Il incombe ainsi aux salariés de veiller aux paramétrages de leurs espaces personnels lorsqu'ils s'expriment sur leur entreprise par le canal de réseaux sociaux.

IV. La protection du droit à l'emploi et les pratiques de recrutement à l'épreuve du numérique

Depuis la fin des années 1990, on assiste à l'essor du « e-recrutement ». De nombreuses innovations en matière d'offre de logiciels de gestion du recrutement permettent désormais de couvrir l'ensemble du cycle de gestion d'un cadre, du moment où il candidate à celui où il devient salarié. L'usage croissant du *Big Data* permet notamment d'identifier les informations les plus pertinentes contenues

74. CA Rouen, 15 novembre 2011, *Mélanie R. c/ Vaubadis*.
75. Cass., 1ère civ., 10 avril 2013 (11-19.530), n° 344.

dans les candidatures. De plus, l'utilisation des réseaux sociaux, donc du partage en temps réel d'éléments de la vie privée ou professionnelle des internautes, fait partie de la vie quotidienne de la plupart d'entre eux. Cependant, les candidats disposent de droits en matière de recrutement (A). La question est de savoir si ces nouvelles pratiques s'inscrivent dans le respect de ces droits (B).

A. Le droit à l'emploi protégé par les droits des candidats en matière de recrutement

En termes de recrutement, le code du travail dispose dans son article 1221-9 qu'« *aucune information concernant personnellement un candidat à emploi ne peut être collectée par un dispositif qui n'a pas été porté préalablement à sa connaissance* ». De plus le candidat doit être informé « *préalablement à leur mise en œuvre, des méthodes et techniques d'aides au recrutement utilisées à son égard* »[76]. Enfin, « *les informations demandées, sous quelque forme que ce soit au candidat à un emploi, ne peuvent avoir comme finalité d'apprécier sa capacité à occuper l'emploi proposé ou ses aptitudes professionnelles* »[77].

La loi « *informatique et libertés* » du 6 janvier 1978 comporte quant à elle de nombreuses dispositions sur la protection du droit à l'emploi. Les applications de gestion du recrutement doivent, préalablement à leur mise en œuvre, faire l'objet d'une déclaration auprès de la CNIL. Cependant, lorsqu'un CIL est désigné, il peut y avoir dispense d'information : « *Les traitements pour lesquels le responsable a désigné un correspondant à la protection des données à caractère personnel chargé d'assurer, d'une manière indépendante, le respect des obligations prévues dans la présente loi sont dispensés de formalités* » [78]. Comme toute personne auprès de laquelle sont recueillies des données à caractère personnel, le candidat dispose d'un droit à l'information, par le responsable du traitement ou son représentant, sur l'identité du responsable du traitement, la finalité poursuivie par le traitement, le caractère obligatoire ou facultatif des réponses, les conséquences à son égard d'un défaut de réponse, les destinataires ou catégories de destinataires des donnée, l'existence d'un droit d'accès et de rectification[79]. Les données à caractère personnel ne peuvent être conservées au-delà de la durée qui n'excède pas celle nécessaire aux finalités pour lesquelles elles sont collectées ou traitées[80], sauf avec l'autorisation de la CNIL. De plus le responsable du traitement automatisé de données doit s'engager envers les candidats à prendre toutes mesures de sécurité et de confidentialité. La CNIL recommande par exemple de ne pas collecter de données relatives à l'origine raciale ou ethnique des employés ou candidats à un emploi et de ne pas procéder à l'analyse de la consonance du nom ou du prénom.

76. Code du travail, article L. 1221-8.
77. Code du travail, article L. 1221-6.
78. Loi du 6 Janvier 1978, article 22.
79. Loi du 6 Janvier 1978, article 32.
80. Loi du 6 Janvier 1978, article 36.

B. Les pratiques de recrutement : réseaux sociaux et applications logicielles

Les pratiques de recrutement sont très diverses. Il existe de multiples sites spécialisés, certains relevant du service public de l'emploi[81], d'autres étant exploités par des entreprises privées[82]. Les plateformes de diffusion multisites permettent aux recruteurs de diffuser en une fois une annonce sur un grand nombre de sites d'emploi.

Par ailleurs, actifs et recruteurs s'accordent sur le fait que les réseaux sociaux professionnels sont devenus des outils importants pour la recherche d'emploi et posent des questions nouvelles quant à la collecte d'informations sur les candidats. Ainsi, l'algorithme de *LinkedIn* se base sur les actions des recruteurs afin de leur proposer « *les utilisateurs qu'ils devraient embaucher* » dans la base de CV du réseau social. Ce service (*Recruiter*) permet de repérer automatiquement les profils, de les ajouter à des listes de candidats potentiels, d'entrer en contact avec les anciens employeurs ou d'être tenu au courant de ceux qui s'attardent sur le profil d'un candidat, sans que les utilisateurs eux-mêmes le sachent. L'utilisateur *lambda* n'a pas accès à la liste de ceux qui ont consulté son profil et les utilisateurs de *Recruiter* peuvent se rendre invisibles.

Par ailleurs, il existe de nombreux outils de sélection des candidatures, notamment des outils informatiques qui vont de l'élaboration de bases de données de suivi *via* des tableurs jusqu'à l'utilisation de systèmes d'information qui gèrent l'ensemble du processus de recrutement (comme des progiciels, des systèmes de gestion de recrutement). Par exemple, certaines entreprises ont recours aux « *job boards* » qui permettent de gérer et de qualifier les candidatures reçues. *Monster* est ainsi capable de déterminer à l'avance combien de candidats devraient postuler à une offre en fonction du bassin d'emploi et de la base de CV.

En outre, la problématique du droit au déréférencement se pose en matière de recrutement, la recherche d'emploi pouvant être entravée de manière significative par une mention défavorable à la personne concernée accessible en ligne. L'arrêt *Google Spain* du 13 mai 2014 de la CJUE, qui consacre le droit au déréférencement, ouvre à cet égard de nouvelles perspectives.

81. www.pole-emploi.fr, www.apec.fr.

82. Par exemple, monster.fr, cadreemploi.fr, keljob.com, eQuest, Career Builder Data Analytics

Contributions

La jurisprudence américaine en matière de liberté d'expression sur Internet, *Winston J. Maxwell, avocat associé, Hogan Lovells*

Des données sans personne : le fétichisme de la donnée à caractère personnel à l'épreuve de l'idéologie des *big data*, *Antoinette Rouvroy, chercheur qualifié au Centre de recherche « Information, droit et société », Faculté de droit de Namur*

Quelle vie privée à l'ère du numérique ?, *Antonio Casilli, maître de conférences à Télécom ParisTech, chercheur en sociologie au Centre Edgar Morin, École des hautes études en sciences sociales*

La jurisprudence américaine en matière de liberté d'expression sur Internet

Par Winston J. Maxwell,
avocat associé, Hogan Lovells

Introduction

La communication via Internet implique plusieurs droits fondamentaux, dont le droit à la protection de la vie privée et la liberté d'expression. Ces deux droits fondamentaux existent aussi bien aux États-Unis qu'en Europe, même si leurs contours précis diffèrent des deux côtés de l'Atlantique. Le présent article examine la liberté d'expression aux États-Unis appliquée à la communication via Internet[83]. Depuis l'affaire *LICRA c/ Yahoo!* en 2000[84] jusqu'à la décision du 13 mai 2014 de la Cour de justice de l'Union européenne (CJUE) dans l'affaire *Google c/ AEPD*[85], le Premier Amendement de la Constitution américaine[86] est souvent perçu comme étant en divergence avec l'approche européenne. Se référant au projet de règlement européen en matière de protection de données personnelles, Rosen (2012) qualifie le droit à l'oubli comme « *la plus grande menace pour la liberté d'expression sur Internet de la prochaine décennie* ».

La présente contribution examine la jurisprudence américaine en matière de liberté d'expression sur Internet, en mettant en exergue les similitudes et les différences avec l'approche européenne.

1. La différence entre l'Internet et la télévision

La décision américaine la plus importante en matière de liberté d'expression sur Internet est *Reno c/ ACLU* (1997)[87]. Cette décision a examiné la constitutionnalité d'une loi[88] qui punissait la mise à disposition de contenus indécents ou sexuellement explicites en ligne, lorsque l'éditeur du contenu savait que ce contenu serait susceptible d'être vu par des mineurs. La ministre de la justice de l'époque, Janet Reno, a soutenu que la loi était conforme au Premier Amendement, puisqu'elle ne visait pas la suppression des contenus, mais seulement l'aménagement d'espaces

83. Pour une analyse de la protection de la vie privée aux États-Unis, voir Maxwell (2014).
84. TGI Paris, 22 mai 2000
85. *Google c/ AEPD*, Cour de justice de l'Union européenne, affaire C 131-12, décision du 13 mai 2014.
86. Le Premier Amendement dispose que « *Le Congrès ne fera aucune loi pour empêcher l'établissement d'une religion, interdire le libre exercice d'une religion ou pour limiter la liberté d'expression, de la presse et des droits des citoyens de se réunir pacifiquement et pour adresser à l'État des pétitions pour obtenir réparations des torts subis* ».
87. 521 U.S. 844 (1997).
88. *Communications Decency Act of 1996*.

sur Internet où ces contenus seraient inaccessibles aux mineurs. Selon la ministre, la loi était comparable à une règle d'urbanisme obligeant les cinémas pour adultes à s'installer dans certains quartiers de la ville. Une loi qui crée seulement des limites à l'emplacement, à la durée ou à la manière de présenter des contenus (*time, place or manner restrictions*) est généralement compatible avec le Premier Amendement. La ministre a également plaidé que la loi était justifiée parce qu'Internet était similaire à la radio ou à la télévision, et que la Cour Suprême a toujours permis une régulation plus contraignante de la télévision et de la radio en raison de leur caractère invasif.

La Cour Suprême n'a pas suivi les arguments de la ministre. La Cour a commencé par souligner la puissance d'Internet comme moyen de communication, en comparant Internet à une tribune où chaque individu peut s'exprimer librement sur une place publique[89]. De plus, la Cour a estimé qu'Internet n'est pas comparable à la radio ou à la télévision, puisque chaque internaute cherche activement le contenu qu'il souhaite, comme lorsqu'il rentre dans une bibliothèque. Contrairement à une émission de radio où les personnes écoutent passivement et peuvent être surprises par un contenu choquant, l'internaute est à la recherche active d'information, et ne sera ni surpris ni choqué par le résultat de ses recherches[90]. L'autre raison pour laquelle Internet n'est pas comparable à la télévision est que l'Internet n'utilise pas le spectre radioélectrique. Contrairement aux chaînes de télévision dont le nombre est limité par la quantité de fréquences de diffusion disponibles, le nombre de sites *web* n'est pas limité par des contraintes techniques. Or c'est la rareté du spectre radioélectrique et l'influence exceptionnelle de la télévision qui justifient une régulation plus stricte de ce média[91]. Pour l'Internet, la Cour a donc écarté l'idée d'une régulation de type audiovisuel en préférant rester sur un mode de régulation légère et très respectueuse de la liberté d'expression, similaire à celle applicable à la presse écrite.

2. Les «*chilling effects*» sur la liberté d'expression

Le point le plus important de la décision *Reno c/ ACLU* concerne les « *chilling effects* », littéralement les « effets réfrigérants », que les tribunaux visent à limiter. Les effets réfrigérants comprennent deux phénomènes. Tout d'abord l'effet de débordement : si une mesure de régulation vise à limiter l'accès à un contenu nocif du type «A», la mesure risque-t-elle également d'avoir un impact sur l'accès aux contenus inoffensifs du type «B»? Dans l'affirmatif, il existe un effet de débordement dommageable à la liberté d'expression. Ensuite, les effets réfrigérants peuvent résulter de la suppression du contenu nocif lui-même : est-ce que la suppression de ce contenu conduira à un appauvrissement général des échanges sur le marché des idées?

---

89. Le Conseil Constitutionnel français a tenu un raisonnement similaire dans sa décision n° 2009-580 DC du 10 juin 2009, paragraphe 12; voir également la décision de la CEDH, *Ahmet Yildirim c. Turquie*, n° 3111/10, du 18 mars 2013.

90. Ce constat est peut-être moins vrai aujourd'hui qu'il ne l'était en 1997, compte tenu notamment de la puissance des moteurs de recherche.

91. *Red Lion Broadcasting c/ FCC*, 395 U.S. 367 (1969). En France, voir Conseil Constitutionnel, décision n° 82-141 DC du 27 juillet 1982, considérant 5.

Plus les effets réfrigérants seront importants, plus la mesure sera en contradiction avec le Premier Amendement. Dans le cas de la loi américaine contestée dans l'affaire *Reno c/ ACLU*, la Cour a identifié deux types d'effets réfrigérants. Premièrement, en visant l'accès à des contenus sexuellement explicites ou indécents, la loi pourrait restreindre l'accès non seulement à la pornographie – le cœur de cible de la mesure – mais également à des informations sur la contraception, sur les maladies sexuellement transmissibles, voire sur l'anatomie. La loi risquerait donc de dépasser sa cible et de freiner l'accès par des mineurs à des informations licites et importantes. Deuxièmement, la loi pourrait conduire les éditeurs de contenus réservés aux adultes à cesser leur activité ou à réduire leur présence sur Internet, par crainte d'être poursuivis pénalement. Puisqu'il est difficile de vérifier l'âge d'un internaute, certains éditeurs préfèreront ne pas prendre le risque d'éditer des contenus pour adultes et cesseront de les rendre disponibles sur Internet. Ainsi les adultes auront accès à moins de contenus pornographiques sur Internet alors que ces contenus sont parfaitement licites pour les adultes. La loi provoquera un appauvrissement dans l'offre de contenus. Pris ensemble, ces deux effets réfrigérants ont rendu la loi non compatible avec le Premier Amendement.

On retrouve le concept d'effet réfrigérant dans le test de proportionnalité appliqué par la CJUE et la CEDH[92]. Lorsqu'elle évalue des mesures prises pour limiter l'accès non autorisé à des œuvres protégées par le droit d'auteur, la CJUE est attentive au moindre effet de débordement qui conduirait à bloquer l'accès à certains contenus non protégés par le droit d'auteur, ou à des contenus protégés par le droit d'auteur mais pour lesquels une exception au droit d'auteur s'appliquerait[93]. En présence d'un effet de débordement, la CJUE aura tendance à juger la mesure excessive par rapport à l'objectif recherché ; la mesure ne passera pas le test de la proportionnalité.

Les effets réfrigérants se retrouvent également dans la littérature concernant la responsabilité des hébergeurs et autres intermédiaires techniques. Dans un régime où l'intermédiaire technique endosse une responsabilité pour le contenu qu'il héberge, Schruers (2002) démontre que l'intermédiaire technique optera pour la prudence : il choisira des contenus et des clients qui présentent des profils de risque faible, ce qui conduira à un appauvrissement général du type de contenus échangés sur Internet.

Le régime spécial de responsabilité des hébergeurs est destiné à remédier à ce problème et à réduire ainsi les effets réfrigérants. Selon ce système, un hébergeur n'est pas responsable du contenu qu'il héberge à condition qu'il retire le contenu rapidement après avoir reçu un signalement. Mais même ce système, favorable aux hébergeurs, n'est pas à l'abri de critiques relatives à ses effets réfrigérants. Si un hébergeur retire un contenu automatiquement dès qu'il reçoit une notification, cela peut conduire à une suppression excessive. Cet effet de débordement a été démontré par *Ahlert* et al. (2004), qui ont adressé des notifications à plusieurs

92. Sur le test de proportionnalité en droit européen, voir Hickman (2008), Sauter (2013) et Tranberg (2011), Callanan *et al*. (2009).

93. CJUE, *Scarlet c/ SABAM*, affaire C 70-10, décision du 24 novembre 2011, paragraphe 52.

plateformes d'hébergement demandant le retrait du texte *De la Liberté* de John Stuart Mill, texte écrit en 1859 et appartenant manifestement au domaine public. Se plaignant d'une prétendue violation du droit d'auteur, la notification a été suivie d'effet par la plupart des hébergeurs situés en Europe, démontrant un « effet réfrigérant » même sous l'égide du régime de responsabilité aménagé. Selon Seltzer (2010) la loi américaine sur le droit d'auteur, le *DMCA*[94], provoque des effets similaires, puisque les notifications de retrait fondées sur le droit d'auteur seront systématiquement suivies d'effet, même si le contenu relève d'un cas d'utilisation équitable (*fair use)*.

3. Les effets réfrigérants et le droit à l'oubli

Les effets réfrigérants seront particulièrement présents en matière de droit à l'oubli. Dans sa décision du 13 mai 2014 contre *Google*[95], la CJUE impose aux moteurs de recherche l'obligation de supprimer certains résultats de recherche à la demande d'une personne concernée, notamment si les informations paraissent anciennes et non pertinentes. Afin de réduire leur responsabilité éventuelle, les prestataires préfèreront donner suite à ces demandes de suppression même lorsqu'il existe un doute quant à leur caractère fondé. Le droit à l'oubli provoquera des effets réfrigérants puisque la mesure affectera non seulement des informations anciennes et non pertinentes, c'est-à-dire celles visées directement par la CJUE, mais également des informations simplement gênantes pour la personne qui a envoyé la notification. En matière de mesures prises pour combattre le téléchargement illicite, la CJUE ne tolère pas d'effet de débordement de ce type[96]. En matière de droit à l'oubli, la Cour semble moins gênée par ces effets collatéraux.

En droit américain, un éventuel droit à l'oubli serait analysé à deux niveaux. Tout d'abord, le cœur de cible de la mesure est-il légitime du point de vue de la liberté d'expression? Une mesure qui vise le retrait de photos ou de vidéos jugées attentatoires à la vie privée serait probablement conforme au Premier Amendement. La liberté d'expression ne protège pas des informations jugées diffamatoires ou attentatoires aux droits d'autrui. En revanche, une mesure visant le déréférencement d'articles de presse qui ne sont pas diffamatoires en soi serait manifestement contraire à la liberté d'expression aux États-Unis.

Deuxièmement, la Cour évaluerait d'éventuels effets de débordement découlant de l'application de la mesure. Si les modalités d'application de la mesure pouvaient conduire à la suppression de contenus en dehors du cœur de cible, la Cour Suprême américaine annulerait la mesure en raison de ses effets réfrigérants. Selon la jurisprudence de la CJUE et de la CEDH, le résultat devrait en principe être identique en Europe compte tenu du test de la proportionnalité. Cependant, la décision de la CJUE du 13 mai 2014 semble s'écarter du test de proportionnalité classique.

---

94. *Digital Millenium Copyright Act* de 1998.
95. CJUE, 13 mai 2014, *Google c/ AEPD*, affaire C 131-12.
96. CJUE, *Scarlet c/ SABAM*, *op. cit.*

Pour Rosen (2012), le droit à l'oubli serait antinomique au Premier Amendement. Si on part du principe qu'un droit à l'oubli du type imposé par la CJUE est contraire au Premier Amendement, on peut s'interroger sur l'effet extraterritorial de la mesure européenne. Une décision de justice rendue en France en matière de droit à l'oubli pourrait-elle être exécutée aux États-Unis ? Cette question rappelle l'affaire *LICRA c/ Yahoo!* de 2000 dans laquelle le tribunal de grande instance de Paris avait ordonné à la plateforme américaine de supprimer l'accès aux objets nazis d'une vente en ligne. Dans une première décision[97], un tribunal californien avait déclaré la décision française contraire au Premier Amendement. Mais la décision d'appel de 2006[98] avait été plus nuancée. Il n'existe pas de convention sur l'exécution des décisions de justice entre la France et les États-Unis. L'exécution d'une décision étrangère est donc régie par des règles de procédure civile de chaque état. Contrairement aux idées reçues, la cour d'appel américaine n'a pas dit qu'elle n'exécuterait pas la décision française contre *Yahoo!*. L'affaire a été rejetée pour d'autres raisons. La cour a expliqué que même si la loi française en question était contraire au Premier Amendement de la Constitution, ce n'est pas pour autant qu'un tribunal américain refuserait son exécution sur le territoire américain lorsque l'application de la loi étrangère viserait à protéger des citoyens français. Pour refuser l'*exequatur*, un tribunal américain doit conclure que l'application de la décision étrangère est fortement incompatible avec les valeurs constitutionnelles américaines[99]. Si les effets de la décision sont cantonnés à un territoire étranger comme la France, un tribunal américain ne refusera pas nécessairement l'exécution de la décision aux États-Unis[100].

4. L'idéologie du « marché des idées »

La liberté d'expression aux États-Unis repose sur une foi quasi absolue dans le bon fonctionnement du « marché des idées ». Lorsque les propos en question s'éloignent du marché des idées, pour se rapprocher d'un acte illégal (par exemple, proférer une menace envers une personne), la liberté d'expression cède la place à la protection d'autres droits et libertés. Pour évaluer la compatibilité des mesures de régulation avec la liberté d'expression, les tribunaux appliquent un test de proportionnalité similaire à celui appliqué par la CJUE et la CEDH. D'un côté, on pèse le préjudice qui sera causé par les propos en question ainsi que la probabilité selon laquelle ce préjudice se réalisera. On tient compte également du caractère imminent du préjudice. De l'autre côté, on évalue le préjudice que la mesure de régulation est susceptible de provoquer elle-même, notamment en faussant le bon fonctionnement du « marché des idées ». Si la mesure en question risque d'étouffer certains points de vue, notamment dans le débat politique, le préjudice causé au marché des idées sera considérable, et ne pourra être justifié qu'en présence d'un préjudice particulièrement important, probable et imminent de l'autre côté de l'équation.

97. *Yahoo!, Inc. v. LICRA*, 169 F. Supp. 2d 1181 (N.D. Cal. 2001).
98. *Yahoo!, Inc. v. LICRA*, 433 F. 3d 1199 (9th Cir. 2006).
99. *Restatement (Third) of Foreign Relations Law* (1987), §482 (2).
100. Ambrose (2013), Maxwell et Coslin (2013).

Posner (2011)[101] résume l'équation comme suit : $B < P \times L / (1 + i)^n$, où :

- B est le coût supporté par la société qui est lié à l'appauvrissement du marché des idées causé par la mesure de régulation proposée, en tenant compte notamment des effets réfrigérants ;

- L est le coût lié à l'événement nocif que la mesure de régulation vise à empêcher, par exemple la commission de crimes racistes ou une attaque terroriste ;

- P est la probabilité selon laquelle l'événement nocif se produira en l'absence de la mesure de régulation ;

- i est le taux d'actualisation ;

- n est le nombre d'années précédant la réalisation de l'événement nocif, en l'absence de la mesure de régulation.

En application de ce test, une mesure interdisant la publication d'informations sur la fabrication d'une bombe chimique artisanale serait justifiée compte tenu de l'ampleur de L. En revanche, une interdiction de propos préconisant le renversement du gouvernement américain ne serait pas justifiée en raison de la faible probabilité P selon laquelle cet événement se produirait, combinée avec le manque d'immédiateté du risque (un «n» élevé). Par ailleurs, le préjudice pour le marché des idées serait élevé puisque la mesure risquerait d'interdire l'échange d'idées politiques dont certaines peuvent se révéler importantes pour le bon fonctionnement de la démocratie. Le même test pourrait être appliqué à une mesure visant à bloquer l'accès à des sites djihadistes. Quelle est la menace réelle de ces sites, et est-ce que cette menace diminuera après la mise en œuvre de la mesure de blocage? Comment distinguer un site djihadiste (le cœur de cible de la mesure) d'un site dédié à l'expression d'un point de vue religieux ou politique important pour le marché des idées? Et surtout, quels sont les effets collatéraux de la mesure sur le marché des idées? Dès 1927, la Cour Suprême reconnaît que pour lutter contre des idées abjectes, « *le meilleur remède est la communication de plus d'idées, non un silence imposé* »[102].

Le principe de confrontation ouverte sur le marché des idées est couplé à un deuxième principe tout aussi important : le gouvernement n'est pas fiable pour faire l'arbitre entre une bonne et une mauvaise idée. Selon cette thèse, le gouvernement aura forcément un conflit d'intérêts, et choisira de supprimer des idées qui constituent une menace pour le pouvoir politique en place. En influant sur le marché des idées, le gouvernement peut ainsi fausser le fonctionnement de la démocratie elle-même, créant un dérapage particulièrement dangereux[103].

---

101. Selon Posner, cette équation traduit le raisonnement de la Cour dans la décision *United States v. Dennis*, 183 F.2d 201 (2d Cir. 1950), *aff'd*, 341 U.S. 494 (1951). L'équation est cependant critiquable car le dommage «B» pourrait également être affecté d'un taux d'actualisation en fonction de son imminence.

102. *Whitney v. California*, 274 U.S. 357 (1927), Brandeis concurring.

103. Breton et Wintrobe (1992).

Coase (1977) souligne certaines incohérences dans ce raisonnement, et suggère que la protection du marché des idées résulte d'un *lobbying* de l'élite intellectuelle, principal « producteur » d'idées affecté par une éventuelle mesure de régulation. Comme tout producteur, l'élite intellectuelle préférera un marché où la production des idées n'est pas limitée. Posner propose une autre explication. La production d'idées nouvelles, surtout lorsqu'elles sont bonnes, demande un investissement. Celui qui crée une nouvelle idée ne bénéficie pas généralement d'un retour sur investissement. Le principal bénéficiaire de l'idée est la collectivité. La fabrication de bonnes idées est donc un bien public, comme la défense nationale. Ainsi, l'État doit encourager la production d'idées, notamment en réduisant des effets réfrigérants tels que des risques de responsabilité pénale.

5. Le Premier Amendement et les discours haineux

Aux États-Unis, une loi interdisant des propos d'incitation à la haine raciale ou religieuse serait contraire au Premier Amendement. Cette conclusion résulte d'une décision de 1992 de la Cour Suprême, dans laquelle la Cour a invalidé un arrêté municipal interdisant le placement d'objets, symboles ou graffiti susceptibles de provoquer la colère ou l'indignation d'autrui en raison de leur race ou de leur religion[104]. L'arrêté municipal visait « notamment » les croix gammées et les croix enflammées. Dans cet arrêt, la Cour Suprême a déclaré incompatible avec le Premier Amendement toute intervention réglementaire qui s'appuie sur le type de contenus communiqués. Les interventions de l'État en matière d'expression d'idées doivent rester neutres par rapport aux points de vue exprimés. En matière de discours haineux, seule une menace immédiate contre des personnes précises peut justifier une interdiction *ex ante*[105].

Waldron (2012) explique que cette position de la Cour Suprême est relativement récente. En 1919, la Cour Suprême a validé une loi punissant la publication de propos soutenant les ennemis des États-Unis. En 1940, le *Smith Act* punit la publication de propos soutenant le renversement du gouvernement. Cette loi a été utilisée pour punir la publication de thèses communistes pendant l'ère McCarthy, avant d'être déclarée contraire à la constitution en 1961[106]. En 1952, la Cour Suprême a validé une loi de l'État de l'Illinois interdisant la publication d'écrits tendant à dénigrer toute classe de citoyens de toute origine ethnique ou religieuse[107], une loi qui n'est pas très éloignée de l'article 24 de la loi du 29 juillet 1881.

Waldron critique la position actuelle de la Cour Suprême à propos du discours haineux, et estime que les tribunaux américains sous-estiment le préjudice causé par les propos racistes, homophobes ou antisémites. Citant les travaux de John Rawls, Waldron estime que l'un des fondements d'une société démocratique est l'existence d'un environnement général de sécurité, de dignité, d'égalité et de respect. Comme l'ordre public, cet environnement serait un préalable nécessaire

104. *R.A.V. v. City of St. Paul*, 505 U.S. 377 (1992).

105. Voir également *Planned Parenthood v. American Coalition of Life Activists* ("the Nuremberg files" *case*), 244 F. 3d 1007 (2001).

106. *Yates v. United States,* 354 U.S. 298 (1957).

107. *Beauharnais v. Illinois*, 343 U.S. 250 (1952).

pour garantir le respect d'autres droits fondamentaux[108]. Waldron compare cet environnement à l'existence d'un air non pollué. Laissé seul, le marché ne produira pas suffisamment d'air pur, puisque l'air pur est un bien public. Une intervention réglementaire est donc nécessaire pour limiter la pollution. De la même manière, une intervention réglementaire serait justifiée pour limiter la prolifération d'images ou de messages dégradants pour certaines classes de la population. Waldron compare la publication de propos racistes à une forme de diffamation contre un groupe de personnes, et soutient que de tels propos peuvent être interdits aux États-Unis sans contrarier le Premier Amendement.

La position de Waldron est minoritaire. Même les ONG de lutte contre la haine raciale et l'antisémitisme aux États-Unis restent méfiantes à l'égard des mesures prises par le gouvernement pour limiter l'expression de certains types d'idées, même abjectes. Ces ONG craignent que ces mesures ouvrent la voie à d'autres mesures attentatoires à la liberté, et plaident plutôt pour une autorégulation au sein des plateformes de l'Internet[109].

6. Internet et le problème de l'anonymat

L'anonymat favorise des propos extrêmes sur Internet. Faut-il interdire l'anonymat sur Internet ?

La question n'est pas simple puisque l'anonymat est un élément de la liberté d'expression aux États-Unis, tout comme en Europe[110]. La Cour Suprême américaine reconnaît que la possibilité d'exprimer des opinions sous couvert d'anonymat est parfois nécessaire afin de protéger l'auteur contre des représailles[111]. Une loi qui interdirait l'anonymat sur Internet serait contraire au Premier Amendement. Sur ce point, le Premier Amendement converge avec le droit à la protection de la vie privée. Comme l'a constaté le rapport indépendant au Président Obama sur les mesures de surveillance massive, une surveillance généralisée des individus sur Internet menace non seulement la protection de la vie privée, mais la liberté d'expression[112]. Ce point a été également soulevé par l'avocat général de la Cour de justice européenne dans l'affaire *Digital Rights Ireland*[113] : la conservation massive de données de connexion par des prestataires d'Internet constitue non seulement une violation du droit à la protection des données personnelles, mais également une violation de la liberté d'expression.

Afin de lutter contre des groupes extrémistes et violents, certains états des États-Unis ont adopté des lois interdisant le port d'un masque dans les rassemblements

108. En matière d'ordre public, on retrouve ce raisonnement dans la décision n° 94-352 du 18 janvier 1995 du Conseil Constitutionnel en matière de vidéosurveillance.
109. Foxman et Wolf (2013).
110. Conseil de l'Europe, Liberté de la Communication sur l'Internet, Principe 7.
111. *McIntyre v. Ohio Elections Commission*, 514 U.S. 334 (1995).
112. *White House* (2013).
113. CJUE, Affaire C-293/12, conclusions de l'avocat général Pedro Cruz Villalon, 12 décembre 2013, paragraphe 52. Dans ses conclusions, l'avocat général cite la jurisprudence de la Cour suprême des États-Unis sur ce point.

publics. Ces lois sont toujours en vigueur et ont été utilisées récemment contre des manifestants du mouvement « *Occupy Wall Street* »[114]. Même si ces lois ont été validées par plusieurs tribunaux[115], Foxman et Wolf (2013) estiment que de telles lois ne pourraient pas être transposées à Internet sans rentrer en conflit avec le Premier Amendement.

La protection de l'anonymat n'est pas absolue. Dans une affaire concernant le téléchargement illégal de musique, la maison de disques *Arista Records* a tenté d'obtenir l'identité de l'internaute suspecté de téléchargement illicite. L'internaute a plaidé qu'il bénéficiait d'un droit à l'anonymat au titre du Premier Amendement de la Constitution. La cour a reconnu que les individus bénéficient d'un droit à l'anonymat au titre du Premier Amendement, mais que ce droit ne peut être utilisé pour commettre des actes illégaux[116]. Le droit à l'anonymat cède en cas de violation des droits d'autrui.

Facebook oblige ses membres à s'inscrire en utilisant leur vrai nom afin notamment de limiter les abus liés à l'anonymat. Foxman et Wolf (2013) citent d'autres exemples de plateformes qui découragent l'anonymat. Un exemple consiste à placer des commentaires non anonymes au-dessus de commentaires anonymes dans les forums de discussion. N'étant pas adossés à une mesure contraignante du gouvernement, ces règlements internes n'entrent pas en conflit avec le Premier Amendement.

7. La liberté d'expression et l'autorégulation

Le Premier Amendement protège le citoyen contre les mesures prises par l'État. Les contrats privés ne sont pas concernés, du moins pas directement. Cela signifie-t-il que les contrats ne peuvent jamais être remis en cause sur le fondement de la liberté d'expression ? Certains auteurs estiment que les contrats peuvent être contestés au titre du Premier Amendement[117].

Cependant, il existe des différences importantes entre des mesures prises par un gouvernement et des mesures prises par des acteurs privés par voie contractuelle. Les acteurs privés agissent généralement dans un contexte de consentement et de concurrence, alors que l'État est en situation de monopole. En matière de liberté d'expression, l'État est considéré comme le monopoleur « le plus dangereux »[118]. La concurrence dans le secteur privé signifie qu'un utilisateur peut changer de plateforme s'il estime que les conditions d'utilisation sont trop restrictives. La

114. S. Gardiner et J. Firger, *«Rare Charge is UnMasked»*, Wall Street Journal Online, 20 septembre 2011, http://online.wsj.com/news/articles/SB10001424053111904194604576581171443151568?mod=e2tw&mg=reno64wsj&url=http%3A%2F%2Fonline.wsj.com%2Farticle%2FSB10001424053111904194604576581171443151568.html%3Fmod%3De2tw.

115. *"*Second Circuit Upholds New York's Anti-Mask Statute against Challenge by Klan-Related Group*", Church of the American Knights of the Ku Klux Klan v. Kerik*, 356 F.3d 197 (2d Cir. 2004), *Harvard Law Review* Vol. 117, n°8 (*June*, 2004), pp. 2777-2784.

116. *Arista Records v. Doe 3*, 2010 WL 1729107 (2d Cir. April 29, 2010).

117. Garfield (1998), Benkler (1999).

118. Posner (2011) p. 931.

situation serait plus complexe si l'ensemble des grandes plateformes adoptait le même règlement interne. Kreimer (2006) a étudié l'utilisation de l'autorégulation sous l'ère McCarthy pour conclure que l'autorégulation peut être un outil redoutable de la censure. Si *YouTube*, *Facebook* et *Twitter* existaient à l'époque de McCarthy, on pourrait imaginer sans trop de difficulté que ces plateformes, sous la pression indirecte du puissant sénateur McCarthy, interdiraient dans leur règlement intérieur tous propos communistes. Dans certains pays non-démocratiques, l'État n'a pas besoin d'adopter une loi pour faire comprendre aux plateformes qu'il convient de bloquer l'accès à certains contenus. L'action de l'État s'exerce par contrainte indirecte sur les acteurs privés. Ce phénomène s'est manifesté après les attaques du 11 septembre 2001[119].

Certaines grandes plateformes Internet interdisent, dans leurs conditions générales d'utilisation, les contenus destinés à provoquer la haine raciale ou religieuse, remplissant ainsi le vide laissé par la jurisprudence. Les plateformes ne surveillent pas les contenus postés par les internautes, mais réagissent aux signalements. Rosen (2013) décrit les personnes qui, au sein des plateformes, sont en charge de gérer les questions délicates de retrait. Ces personnes, appelées les « décideurs », ont, selon le professeur Rosen, plus d'impact sur les types de contenus visibles sur Internet que les juges et les autorités de régulation. Les plateformes ont créé un groupe de travail sur les contenus haineux présents sur Internet (*Anti Cyber HateWorking Group*) dont les objectifs sont de développer des méthodes qui permettent aux plateformes de se positionner vis-à-vis de contenus controversés tels que la vidéo « *L'innocence des musulmans* » postée sur *YouTube* (qui a provoqué des émeutes et même l'intervention du Président Obama devant les Nations Unies). Un autre exemple cité par le professeur Rosen est l'échange de *tweets* antisémites dans l'affaire « #Unbonjuif ».

Les plateformes emploient un réseau de personnes qui évaluent les signalements dans un premier temps et déterminent ceux qui doivent donner lieu à un retrait instantané et ceux qui doivent être soumis à leur superviseur chargé de s'assurer du respect des politiques de contenus. Des contenus qui poussent à la violence de manière précise, envers un groupe de personnes bien déterminé, sont généralement enlevés. En revanche, des contenus qui critiquent une institution, un État ou une religion de manière générale ne sont pas enlevés immédiatement. Si le contenu est manifestement illégal dans un pays donné, par exemple les *tweets* « #Unbonjuif » en France, l'accès au contenu dans ce pays peut être bloqué si la technologie le permet.

Rosen parvient à la conclusion que la méthodologie appliquée par les plateformes, bien qu'étant imparfaite, aboutit à des résultats qui ne sont pas très éloignés de ce qu'aurait décidé un tribunal confronté au même problème de contradiction entre les lois de différents pays. Il s'agit ainsi d'une forme d'autorégulation qui permet de trouver un équilibre prenant en compte des considérations à la fois juridiques et pragmatiques.

119. Maxwell et Massaloux (2002).

8. Peut-on envisager un régulateur de la liberté d'expression ?

Le régulateur naturel de la liberté d'expression aux États-Unis est le tribunal. Il revient à la Cour suprême des États-Unis de fixer les grands principes qui permettent d'établir l'équilibre entre le Premier Amendement et la protection d'autres droits. Les tribunaux inférieurs appliquent ensuite ces principes aux cas qui leur sont soumis. Serait-il possible de confier cette tâche à un régulateur autre qu'un tribunal?

La Cour suprême a évoqué cette question en 1965, en décidant qu'une loi prévoyant l'obtention d'un visa administratif pour la sortie d'un film était contraire au Premier Amendement si la loi ne prévoyait pas la possibilité d'un recours immédiat devant un tribunal en cas de refus[120]. La Cour a déterminé qu'en matière de liberté d'expression, seul un tribunal peut imposer une mesure définitive limitant la liberté d'expression. Selon la Cour, une autorité administrative manque d'indépendance par rapport aux pressions politiques et ne pourra jamais être aussi neutre et impartiale qu'un tribunal. De plus, une autorité administrative risque d'être influencée par sa propre pratique administrative et souffrira d'un champ de vision étriqué. Cela ne signifie pas pour autant qu'un tribunal doit forcément être le décideur de premier ressort. Une autorité administrative peut prendre une première décision, à condition que cette décision puisse immédiatement faire l'objet d'un appel devant un tribunal[121]. Monaghan (1970) appelle ces règles les « *garanties procédurales du Premier Amendement* ».

La loi américaine sur le droit d'auteur a confié à une autorité administrative le soin de fixer des règles en matière de mesures techniques de protection. L'objectif du régulateur est de trouver un équilibre entre la protection effective du droit d'auteur et la liberté d'expression. En particulier, le régulateur doit s'assurer que les mesures techniques de protection n'enfreignent pas le droit à l'utilisation équitable (*fair use*) des œuvres. Le régulateur adopte ses décisions après consultation publique, et ses décisions peuvent être contestées devant les tribunaux. Cette autorité de régulation américaine traite incontestablement des sujets liés à la liberté d'expression[122].

Le régulateur américain de l'audiovisuel, la *Federal Communications Commission (FCC)*, prend également des décisions limitant la liberté d'expression. En particulier, le régulateur américain sanctionne des chaînes de télévision qui diffusent des contenus « indécents » pendant les heures de grande écoute. L'incident le plus connu est l'amende de $550 000 imposée par la *FCC* en raison du « dysfonctionnement vestimentaire » de Janet Jackson lors du *Super Bowl* américain de 2004. L'amende a été annulée par les tribunaux.[123]La Cour suprême a récemment invalidé d'autres amendes puisque la *FCC* n'avait pas informé les chaînes suffisamment à l'avance

120. *Freedman v. Maryland,* 380 U.S. 51 (1965).

121. Dans sa décision n° 2009-580 DC du 10 juin 2009, le Conseil constitutionnel a décidé que la suspension d'un accès à l'internet ne pouvait être décidée en premier ressort par une autorité administrative.

122. Liu (2004), Maxwell (2013).

123. *CBS Corp. v. FCC*, No. 06-3575 (3d Cir. Nov. 2, 2011).

de son changement de doctrine en matière de contenus indécents[124]. Cependant, la Cour suprême n'a pas remis en cause le pouvoir de la *FCC* pour réguler ces questions, confirmant là-encore la possibilité pour une autorité de régulation d'agir en matière de liberté d'expression, à condition bien sûr qu'il existe la possibilité de faire appel de la décision rapidement devant les tribunaux.

Conclusion

Les tribunaux des États-Unis considèrent l'Internet comme un médium d'expression méritant le plus haut degré de protection au titre du Premier Amendement. Pour ces tribunaux, publier un contenu sur Internet est l'équivalent de la distribution de tracts sur une place publique. L'État peut organiser les modalités de la distribution de tracts, mais ne peut pas, sauf à de rares exceptions, censurer le type de contenu exprimé dans les tracts. Toute régulation doit rester neutre par rapport au point de vue exprimé. Selon la Cour suprême, le meilleur moyen de combattre des idées abjectes est de favoriser la publication d'autres idées qui viendront les concurrencer. Ainsi, un site Internet qui contient des propos d'incitation à la haine raciale sera protégé par le Premier Amendement, sauf si les propos contiennent une menace immédiate contre des personnes précises. Les tribunaux américains appliquent un test de proportionnalité similaire à celui appliqué en Europe, mais accordent une importance particulière aux dommages collatéraux (*chilling effects*) qui peuvent être provoqués par une loi ou un règlement limitant la liberté d'expression sur Internet.

Dans leur règlement intérieur, les grandes plateformes de l'Internet interdisent la publication de propos d'incitation à la haine raciale. Ces règlements intérieurs viennent ainsi combler le vide laissé par la jurisprudence. Certaines plateformes limitent également l'anonymat des internautes, même si – là encore – la jurisprudence reconnaît un certain droit à l'anonymat au titre du Premier Amendement. Adopté peu de temps après la Révolution américaine, le Premier Amendement traduit surtout une méfiance à l'égard de l'État. Les Américains estiment que l'État ne peut pas agir en tant qu'arbitre dans le marché des idées car il pourrait fausser le jeu à son avantage et dérégler ainsi le fonctionnement de la démocratie. C'est pour cela que les Américains privilégient l'autorégulation pour limiter la disponibilité de contenu abject sur l'Internet. L'autorégulation n'est certes pas parfaite, car elle fournit peu de garanties procédurales. Cependant, l'autorégulation est perçue comme étant préférable à une régulation de l'État en raison du risque de détournement que représente l'implication de l'État dans cette délicate question.

124. *Fox Television v. FCC*, 132 S. Ct. 2307 (2012).

Références

Ahlert, C., Chris Marsden and Chester Yung (2004), "How 'Liberty' Disappeared from Cyberspace: The Mystery Shopper Tests internet Content Self-Regulation" http:/pcmlp.socleg.ox.ac.uk/text/liberty.pdf.

Ambrose, M. L. (2013), "Speaking of Forgetting: Analysis of Possible Non-EU Responses to the Right to Be Forgotten and Speech Exception", *TPRC Conferences, TPRC 41: The 41st Research Conference on Communication, Information and Internet Policy. Available at SSRN:* http://ssrn.com/abstract=2238602 *or* http://dx.doi.org/10.2139/ssrn.2238602.

Benkler, Y. (1999), "Free as the Air to Common Use: First Amendment Constraints on Enclosure of the Public Domain", *74 N.Y.U. L. Rev. 354.*

Breton, A. and R. Wintrobe (1992), "Freedom of speech vs. efficient regulation in markets for ideas", *17 J. of Econ.Behavior and Organization 217.*

Callanan, C., M. Gercke, E. De Marco and H. Driez-Ziekenheiner (2009), "Internet Blocking – Balancing Cybercrime Responses in Democratic Societies", http://www.aconite.com/sites/default/files/Internet_blocking_and_Democracy.pdf.

Coase, R.H. (1977), "Advertising and Free Speech", *6 J. of Leg. Studies 1.*

Foxman, A. and C. Wolf (2013), "Viral Hate – Containing its Spread on the Internet", *Palgrave Macmillan.*

Garfield, A. (1998), "Promises of Silence: Contract Law and Freedom of Speech", *83 Cornell L. Rev. 261*.

Hickman, T. (2008), "The Substance and Structure of Proportionality", *Public Law 694.*

Kreimer, S. (2006), "Censorship by Proxy: The First Amendment, Internet Intermediaries, and the Problem of the Weakest Link", *155 Penn. L. Rev. 11.*

Liu, J. (2004), "Regulatory Copyright", *83 North Carolina L. Rev. 87.*

Maxwell, W. and J. Massaloux (2002), "Freedom of Speech and the Internet: European and US Perspectives after September 11th, 2001", *47 Comm. &Strategies 121*.

Maxwell, W. (2013), «Exceptions au droit d'auteur: deux modèles outre-Atlantique», *Rev. Lamy Droit de l'Immatériel*, n° 94, juin.

Maxwell, W. (2014)*,* «La protection des données à caractère personnel aux États-Unis: convergences et divergences avec l'approche européenne», dans «Le cloudcomputing», *Société de législation comparée, collection colloques* v. 22.

Maxwell, W. and C. Coslin (2014), «L'efficacité à l'étranger des décisions françaises en matière de communication : le cas des États-Unis et du Premier Amendement», Légicom n° 52.

Monaghan, H.P. (1970), "First Amendment 'Due Process'", *83 Harvard L. Rev. 518.*

Posner, R.A. (2011), "Economic Analysis of Law", *Aspen Casebook Series, 8th Edition*.

Rosen, J. (2012), "The Right to be Forgotten", *64 Stan. L. Rev. Online 88.*

Rosen, J. (2013), "The Delete Squad",*The New Republic, 29 April.*

Sauter, W. (2013), "Proportionality in EU law: a balancing act?", *TILEC Discussion Paper DP 2013-0003.*

Seltzer, W. (2010), "Free Speech Unmoored in Copyright's Safe Harbor: Chilling Effects of the DMCA on the First Amendment", *24 Harvard J. L.& Technology 171*.

Singh, A. (2011), "Agency Regulation in Copyright Law: Rulemaking under the DMCA and its broader implications", *26 Berkeley Technology L. J. 527.*

Tranberg, C.B. (2011), "Proportionality and data protection in the case law of the European Court of Justice", *1 Inter. Data Privacy L. 239.*

Waldron, J. (2012), "The Harm in Hate Speech", *Harvard U. Press.*

White House (2013), "Liberty and Security in a Changing World, Report and Recommendations of The President's Review Group on Intelligence and Communications Technologies", http://www.whitehouse.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf.

Des données sans personne : le fétichisme de la donnée à caractère personnel à l'épreuve de l'idéologie des *big data*

Par Antoinette Rouvroy,
chercheur qualifié au Centre de recherche
« Information, droit et société »,
Faculté de droit de Namur

Parcourue par des logiques de flux et de valorisation des flux, notre époque semble marquée par une « explosion » des volumes de données numériques, reflétant le monde jusque dans ses moindres événements sous une forme éclatée, segmentée, distribuée, décontextualisée, déhistoricisée, ou, pour le dire autrement, sous forme de données individuellement a-signifiantes mais quantifiables, opérant comme de purs signaux en provenance du monde connecté, métabolisables à grande vitesse par les systèmes informatiques. L'enregistrement systématique et par défaut de quantités massives de données numériques et les nouvelles possibilités d'agrégation de ces données (*datamining*) met à disposition des autorités publiques et des entreprises privées une nouvelle sorte de « savoir », fondé sur des données triviales, pas nécessairement privées par nature, mais qui, en raison de leur quantité (plus que de leur qualité), nous exposent individuellement et collectivement à une série de risques inédits, irréductibles aux enjeux de protection de la vie privée et de protection des données à caractère personnel[125]. C'est de quelques-uns de ces risques inédits que nous voudrions esquisser ici une amorce de diagnostic.

1. Une carte sans territoire

L'univers numérique se compose, dit-on, de plus de mille-deux-cent milliards de milliards d'octets, dont quatre-vingt-dix pourcents auraient été produits dans les deux dernières années, et dont le nombre devrait être multiplié par dix d'ici 2020 en raison de la mise en réseau d'un nombre croissant d'objets équipés de puces RFID et capables de communiquer entre eux, et donc de produire, eux aussi, des quantités gigantesques de données[126].

Il nous est difficile de nous *représenter* cette gigantesque carte sans territoire. À dire vrai, *Big Data* signifie surtout le franchissement d'un seuil à partir duquel nous serions contraints (par la quantité, la complexité, la rapidité de prolifération des données) d'abandonner les ambitions de la rationalité moderne consistant à relier les phénomènes à leurs causes, au profit d'une rationalité que l'on pourrait dire post-moderne, indifférente à la causalité, purement statistique,

125. À cet égard, lire notamment Gray, David C. and Citron, Danielle Keats, « A Technology-Centered Approach to Quantitative Privacy », 14 août 2012. SSRN: http://ssrn.com/abstract=2129439.
126. http://france.emc.com/leadership/digital-universe/index.htm

inductive, se bornant à repérer des *patterns*, c'est-à-dire des motifs formés par les corrélations observées entre des données indépendamment de toute explication causale. La répétition de ces « motifs » au sein de grandes quantités de données leur confère une valeur prédictive. Ainsi voit-on apparaître grâce à la visualisation algorithmique des relations subtiles (des relations qui n'auraient pas été perceptibles autrement) entre les données un tout nouveau type de « savoir », exploitable dans une multitude de domaines (astronomie, climatologie, épidémiologie, sciences sociales[127], économie et finance[128]…). L'« intelligence » des algorithmes consiste en leur capacité à traiter statistiquement ces quantités massives, complexes, relativement peu structurées, de données dans un temps record, pour en faire surgir non pas des relations causales explicatives mais des corrélations statistiquement signifiantes entre des éléments a priori sans rapport, c'est-à-dire des profils exploitables notamment pour détecter, sans avoir à les rencontrer ni à les interroger personnellement, les risques et opportunités dont sont porteuses des personnes. Devient alors actuel par avance ce qui n'existait que sur le mode de la potentialité. Le domaine d'application qui nous intéressera ici, bien sûr, sera celui de la modélisation ou du profilage des comportements humains à des fins diverses sur la base des données émanant des individus, des contextes dans lesquels ils vivent, ou produites automatiquement.

2. Un univers sans sujet ni forme

À la différence du monde physique, l'univers numérique, déterritorialisé, n'est peuplé d'aucun objet, d'aucune forme résiliente, mais seulement de réseaux de données. *A fortiori*, aucun corps individuel, subjectif, actuel, susceptible d'événement, ne s'y peut rencontrer. L'unique sujet qui est aussi l'unique souverain de l'univers numérique est un corps statistique, impersonnel, virtuel, moulage générique et changeant des « risques et opportunités » détectés en temps réel, nourris de fragments infra-personnels d'existences quotidiennes agrégés à un niveau supra-individuel sous forme de modèles de comportements, ou profils, auxquels correspondent, par certaines combinaisons de traits chaque fois spécifiques, une multitude de personnes. Aussi ne sommes-nous bien souvent même plus identifiables comme auteurs ni émetteurs des données « qui comptent » et qui nous gouvernent : les « données brutes », lesquelles sont de fait soigneusement nettoyées des traces de leur contexte originaire et de toute signification singulière.

---

127. Pour une critique de l'exploitation des *Big Data* pour la recherche en sciences sociales, voir les travaux de Dominique Cardon.

128. Les algorithmes de *trading* à haute fréquence exécutent des transactions financières sur la base de recommandations faites par des algorithmes statistiques capables de détecter les fluctuations boursières avant qu'elle ne se produisent et d'y « réagir par avance » en quelques microsecondes. Au point que l'on pourrait se demander dans quelle mesure la rapidité de détection et de réaction pourrait évoquer le délit d'initié (je remercie pour cette suggestion stimulante Jérémy Grosman, doctorant au Centre de Recherche en Information, Droit et Société de l'Université de Namur).

Il en résulte que, contrairement à l'intuition majoritaire, nous n'avons peut-être jamais été, dans nos singularités respectives, moins *significativement* visibles que dans l'univers numérique. D'ailleurs, qui nous sommes singulièrement, quelle est notre histoire, quels sont nos rêves, quels sont nos projets – ces dimensions *autobiographiques* de nos personnes inaccessibles dans l'actualité pure de l'immédiateté - tout cela intéresse sans doute, dans des proportions variables, nos « amis » des réseaux dits sociaux, mais cela n'intéresse fondamentalement ni *Google*, ni *Facebook*, ni la NSA, ni *Amazon*, ni aucun de ceux qui nous « gouvernent ». Nous n'intéressons plus tous ceux-là, et d'autres encore, qu'en tant qu'agrégats temporaires de données exploitables en masse, à l'échelle industrielle, une fois décontextualisées, purifiées de tout ce qui aurait pu les rattacher à ce qui fait la singularité d'une vie. Pour construire un « profil » - afin de pouvoir « capitaliser » sur les risques et opportunités dont nous sommes porteurs - les données de nos voisins sont aussi bonnes que les nôtres. Comme les « modèles » ou « profils » sont construits, au départ, de données en provenance de grandes quantités d'individus et que les données relatives à l'un des individus sont tout aussi (peu) signifiantes que celles d'un autre pour la modélisation ; des données très peu personnelles, en très petite quantité, suffisent à produire à l'égard de n'importe quel individu des savoirs « nouveaux », c'est-à-dire à inférer certains éléments sans rapport immédiat avec les données « qui le concernent » mais qui permettent néanmoins de le « cataloguer »[129]. Nous ne faisons plus « autorité » en tant qu'individus, pour rendre compte de nous-mêmes face au profilage algorithmique[130]. « *Ce qui est réel – pour autant que l'on puisse supposer qu'une telle chose existe en elle-même – n'importe pas ; ce qui importe est ce que l'on tient pour réel et dans la modernité ce que l'on tient pour réel est statistiquement enregistré* »[131].

On pourrait d'ailleurs faire l'hypothèse suivant laquelle ce serait en partie en raison de la chute spectaculaire du cours du récit, de l'expérience, du témoignage singulier, du *non numérisable* dans les rapports que les individus peuvent avoir avec les bureaucraties tant privées que publiques (au profit d'un profilage plus ou moins systématique, plus ou moins automatique, dispensant de toute rencontre et de tout échange langagier), que se reportent dans l'espace des réseaux sociaux les performances identitaires ne trouvant plus à s'épanouir ailleurs. Après tout peut-être les pages personnelles, les murs *Facebook* et les comptes *Twitter* ne sont-ils rien d'autre que les avatars contemporains de l'intérieur bourgeois de la fin du 19ème siècle décrit par Walter Benjamin, dans lequel « *il n'est pas de recoin où*

129. Martijn van Otterlo, « Counting Sheep: Automated Profiling, Predictions and Control », contribution à l'*Amsterdam Privacy Conference* des 7-10 octobre 2012.

130. C'est que cette « autorité », cette responsabilité de choisir et d'énoncer, nous serions prêts à la sous-traiter à des machines "intelligentes". C'est en tous les cas ce que pense Erik Schmidt, patron de *Google* : "En fait je pense que ce que veulent la plupart des gens, ce n'est pas que *Google* réponde à leurs questions mais leur dise ce qu'ils devraient faire", confiait-il dans une interview publiée au *Wall Street Journal* (Interview par Holman W. Jenkins Jr., « Google and the Search for the Future. The Web icon's CEO on the mobile computing revolution, the future of newspapers, and privacy in the digital age. », *Wall Street Journal*, 14 août 2010)

131. Skouteris, « Statistical Societies of Interchangeable Lives », *Law and Critique*, 2004, vol.15, n.2, p.15.

l'habitant n'ait déjà laissé sa trace : sur les corniches avec ses bibelots, sur le fauteuil capitonné avec ses napperons, sur les fenêtres avec ses transparents, devant la cheminée avec son pare-étincelles[132] ». Quelle meilleure manière en effet, pour se consoler de l'anonymat ou de l'insignifiance dans l'espace public, que de saturer son espace privé (autrefois) ou ses pages dites personnelles sur Internet de traces témoignant de son passage terrestre et de son statut social ?

3. Une mémoire par défaut

La rétention par défaut des données transpirant de l'activité humaine

La numérisation de la vie même – qui en est aussi, dans une certaine mesure, une disqualification – résulte en partie seulement de l'exposition plus ou moins (in)volontaire de ceux que l'on appelle les internautes sur les réseaux dits sociaux, les blogs, et autres plateformes de l'Internet. Une partie des données sont donc « produites » ou « coproduites » par les individus, soit sciemment (lorsqu'ils génèrent du contenu sur Internet par exemple), soit à leur insu (lorsque leurs activités, interactions, trajectoires, sont enregistrées sous une forme numérique par des caméras de surveillance, par des dispositifs de géolocalisation, etc.).

En raison notamment des réglages par défaut des appareils numériques et des logiciels d'applications (qui conservent par exemple l'historique des recherches sur les moteurs de recherche à moins que l'utilisateur ne manifeste expressément sa volonté de ne pas conserver d'historique), c'est plutôt sur le mode de l'adhésion par défaut que du consentement libre et éclairé que les individus vivent cette prolifération des données enregistrées « dans les nuages », c'est-à-dire très loin de l'appareil de l'utilisateur, mais contrairement à ce qu'évoque la métaphore nébuleuse, non pas de façon distribuée mais dans d'une manière très centralisée dans de gigantesques *datacenters*.

Le succès des règles de conservation des données par défaut ou, pour le dire autrement, le manque de succès des options permettant de déroger à cette règle de conservation des données tient, si l'on en croit Cass R. Sunstein, se fondant sur l'économie comportementale, à la combinaison de trois facteurs principaux : 1) Le premier facteur est l'inertie des comportements dès lors qu'effacer « ses traces » demande un effort dont on ne sait au juste s'il vaut vraiment la peine, étant donné que chacune des données émanant de nos activités en ligne nous paraît à nous-mêmes, *a priori* (indépendamment des opérations de recoupement, de croisement, de modélisation auxquelles elles pourraient contribuer), de peu d'importance. La règle par défaut, quand bien même nous avons la possibilité d'y déroger très facilement « en quelques clics » prévaudra toujours lorsque l'enjeu ponctuel, actuel, n'apparaît pas significatif aux yeux de l'internaute. 2) Le second facteur favorisant la règle de conservation par défaut consiste en ceci que, dans une situation d'incertitude quant à la marche à suivre, l'utilisateur moyen aura tendance à considérer que la règle par défaut, puisqu'elle a été pensée par d'autres que lui, réputés plus experts et puisqu'elle est probablement suivie par la plupart des autres personnes, est sans doute la meilleure option pour lui aussi. 3) Enfin,

132. W. Benjamin, "Expérience et pauvreté", 1933.

le troisième facteur consiste dans le fait que les individus soient généralement plus sensibles au risque de perdre un avantage dont ils ont ou croient avoir la jouissance en se maintenant dans la situation dans laquelle ils se trouvent qu'à l'opportunité de gagner quelque chose en changeant. C'est une variante du phénomène d'inertie mais à travers laquelle les concepteurs, des « designeurs », les « marketeurs » peuvent avoir une prise sur les individus : ils peuvent réduire la probabilité que les utilisateurs s'écartent de la règle par défaut dans l'ajustement des « règles de confidentialité » en évoquant tout ce qu'ils ont à perdre dans la mesure où la rétention des « traces numériques » est ce qui permet de leur offrir un service plus personnalisé, plus adapté à leurs besoins en temps réel en fonction du lieu où ils se trouvent, ou de leurs goûts, un service plus rapide et efficace, et que l'effacement leur fera *perdre* tous ces avantages suffira généralement à éviter que l'utilisateur ne s'écarte de la règle par défaut[133].

Parce que l'autonomie individuelle, pour peu qu'elle existe, n'est pas une capacité purement psychique, mais qu'elle dépend de facteurs socio-économiques, éducatifs, de « design », les « architectures » du choix individuel – telles que les systèmes de règles par défaut – fondées sur des acquis de la psychologie sociale ou sur une détection algorithmique du profil psychologique de celui qu'on appelle l'utilisateur, devraient faire l'objet d'évaluations rigoureuses, spécialement lorsqu'elles sont l'œuvre d'acteurs dont les intérêts ne sont pas alignés sur ceux des « utilisateurs ». Nous ne saurions trop insister sur l'urgence de procéder à une typologie des acteurs du « numérique » et surtout de leurs « intérêts ». Cette voie nous semble plus prometteuse à l'heure actuelle qu'un arc-boutement de principe sur l'exigence illusoire d'un consentement libre et éclairé. Les architectures de choix construites par des acteurs dont les intérêts ne sont pas alignés sur ceux de l'utilisateur, incitant, par les moyens décrits plus haut, l'utilisateur à ne pas s'écarter de la règle par défaut, d'être en pratique incompatible avec ce qu'Henri Atlan, par exemple, appelle « l'expérience minimale du choix » qui « implique que plusieurs alternatives soient offertes et que le choix soit le facteur déterminant par lequel l'une d'entre elles est réalisée, passant ainsi du statut de possible à celui de réel, ou, plus précisément, d'actuel. En effet, cette expérience implique que l'ensemble des possibles ait une certaine forme de réalité, d'existence en tant que possibles, avant que l'un d'entre eux soit actualise. Que le choix lui-même ait été déterminé par des causes que nous ne connaissons pas et qu'il nous semble "libre" au sens de non contraint pour cette raison, n'empêche pas que nous fassions l'expérience de cette existence des possibles et de l'actualisation de l'un d'entre eux, consécutive – temporellement et causalement – au choix que nous faisons. C'est pourquoi la nature de la réalité et des choix impose que l'on se pose la question de «*la nature du possible non actualisé et de la réalité de son existence*.»[134]

Il nous semble, quoi qu'il en soit, que la règle par défaut prévaudra dans la plupart des cas, à moins que les internautes aient pris conscience, collectivement, de tout ce qu'ils ont à gagner, non en terme de confort, mais en termes de puissance d'agir,

133. Cass R. Sunstein, « Impersonal Default Rules vs. Active Choices vs. Personalized Default Rules : A Triptych », 19 mai 2013, http://ssrn.com/abstract=2171343

134. Henri Atlan, *Les étincelles de hasard,* T. 2., Seuil, 2003, *p*. 77.

en s'en écartant et en effaçant leurs traces : non seulement un vague sentiment d'anonymat rassurant, mais la possibilité de n'être pas (trop) *p*rofilés, de n'être pas toujours déjà là où ils sont attendus, de voir, de lire, de consommer des choses qui n'auront pas été prévues pour eux, de n'être pas toujours déjà enfermés dans une bulle immunitaire hyper-personnalisée, mais, au contraire, d'être exposés et de participer à l'espace public en formant et en énonçant par eux-mêmes et pour autrui leurs motivations, leurs désirs, leurs raisons, leurs intentions, leurs projets, plutôt que de sous-traiter à des machines le soin de personnaliser par avance leur environnement de telle manière qu'ils n'aient plus même à former pour eux-mêmes et à formuler pour leurs contemporains ce qu'ils pourraient bien désirer.

Par ailleurs, si l'on conçoit aisément que les données, y compris les données à caractère personnel, puissent être conservées et traitées lorsqu'elles sont nécessaires à la fourniture d'un service déterminé, et, précisément, personnalisant, il se pourrait fort bien que de nombreux opérateurs enregistrent et conservent des données en excès de ce qui serait strictement nécessaire aux services dont ils gratifient leur clientèle. Ainsi, la géolocalisation continue des utilisateurs ne peut être justifiée en dehors des moments où l'utilisateur utiliserait spécifiquement certaines applications (la recommandation automatisée de restaurants à proximité de là où il se trouve par exemple) nécessitant la géolocalisation, mais il est de fait extrêmement difficile pour un utilisateur de s'assurer que ses données sont traitées conformément aux engagements spécifiques de l'opérateur et en conformité avec la législation en vigueur, car, bien sûr, rien de tout cela ne se voit ni ne s'éprouve. Le principe de minimisation des données est donc systématiquement mis à mal, d'autant que, dans l'idéologie des *Big Data*, toute donnée triviale, y compris ce qui passerait, dans le contexte de traitements statistiques plus classiques, pour du « bruit », peut concourir à la production de profils.

De même, il est douteux que les utilisateurs de certains réseaux sociaux, en donnant leur consentement formel à la conservation et à l'exploitation de leurs données à des fins de recherche et d'amélioration des fonctionnalités du réseau aient réellement voulu donner la permission de se servir d'eux comme « cobayes » pour des expériences de psychologie sociale menées sur ce réseau et consistant à tenter de manipuler leurs émotions en triant, pendant un certain temps, le « fil d'actualités » auxquels ils étaient exposés de manière à étudier l'incidence, sur leur humeur, d'une exposition relativement prolongée à des expressions plutôt pessimistes, négatives, alarmistes, etc. C'est, cette fois, le principe de finalité qui se trouve mis à mal. Mais ce dernier est bien sûr également incompatible avec l'idéologie des *Big Data*, en cela soutenue par l'impératif de l'innovation érigé au rang de logique absolue.

Les données transpirant des objets communicants et les métadonnées

À toutes ces données émanant directement de l'activité humaine (aujourd'hui, lorsque nous travaillons, consommons, nous déplaçons, nous « produisons » presqu'inévitablement de la donnée), s'ajoutent les données produites par les objets, de plus en plus nombreux, reliés à l'« Internet des objets », ainsi que les métadonnées, c'est-à-dire des données générées automatiquement et relatives

au contexte des transactions et communications opérées via Internet : les dates et heures auxquelles ont lieu les transactions ou communications, les adresses IP des appareils de l'expéditeur et du destinataire, le lieu où une personne se trouvait la dernière fois qu'elle a relevé son courriel… il s'agit d'informations transactionnelles et contextuelles à l'exclusion des contenus et des détails relatifs aux personnes. Les métadonnées ne font donc pas partie de la catégorie des données à caractère personnel[135] et échappent de ce fait au champ d'application des régimes européens de protection des données à caractère personnel. Bref, contrairement à ce que pourrait laisser croire un certain fétichisme de la donnée à caractère personnel, celle-ci n'occupe, dans l'univers numérique, qu'une place de plus en plus anecdotique. De plus, l'opposition entre données personnelles et données anonymes tend à s'estomper en raison des diverses techniques de « ré-identification » d'individus au départ de données anonymes (leurs données de connexion, la suite de leurs localisations GPS…). De la même manière, les possibilités de croisement de données (de consommation, de localisation, de navigation sur Internet…) anonymes permet de générer à propos des personnes des informations sensibles (état de santé actuel ou futur, préférences sexuelles, convictions religieuses, opinions politiques…). Ce sont toutes les catégories de données intervenant dans les régimes juridiques de protection des données à caractère personnel qui se trouvent perdre en pertinence pour les objectifs de protection qui sont les leurs.

4. Un nouveau régime de vérité : le réel *comme tel*

Cette explosion des données, et la sorte de comportementalisme numérique qui l'accompagne, instaure un nouveau « régime de vérité »[136] numérique, une nouvelle manière de rendre le monde signifiant : la « réalité » (ou ce qui en tient lieu) y serait saisie – à en croire l'idéologie des *Big Data* – non plus au niveau de ses représentations et transcriptions ou de ses interprétations individuelles ou collectives, mais au niveau quasiment atomique ou génétique de la « donnée », considérée comme un fait ultime, parlant d'elle-même sans médiation, dans un langage objectif situé au degré zéro de l'écriture, un langage constitué de suites interminables de 1 et de 0.

C'est l'utopie d'un accès immédiat au réel comme tel, à travers son « double » numérisé, et d'une modélisation anticipative du monde à même le monde numérisé

135. Nous n'entrerons pas ici dans les détails de la controverse relative à la qualification de l'adresse IP comme donnée à caractère personnel.

136. C'est-à-dire de nouvelles manières, ou de nouveaux processus, à travers lesquels s'établit ce que l'on tient pour vrai. "(…) *pourquoi en effet ne pas parler de régime de vérité pour désigner l'ensemble des procédés et institutions par lesquels les individus sont engagés et contraints à poser, dans certaines conditions et avec certains effets, des actes bien définis de vérité ? Pourquoi après tout ne pas parler des obligations de vérité comme [on parle] des contraintes politiques ou des obligations juridiques ?* (…) *Il y aurait des obligations de vérité qui imposeraient des actes de croyance, des professions de foi [ou] des aveux à fonction purificatrice*." (M. Foucault, Le gouvernement des vivants, Cours au Collège de France, 1979-1980, EHESS, Gallimard, Seuil, 2012, p.92.)

lui-même[137], transcendant toutes les formes instituées. Cette *naturalisation* de la « donnée » – qui a l'air d'émaner tellement directement du monde tel qu'il est qu'elle rendrait, selon certains, toute modélisation, toute théorie obsolète[138] – est bien sûr idéologique. Le « savoir » produit par le *datamining* apparaît particulièrement « neutre » : il n'apparaît pas comme le résultat de rapports de pouvoir et ne paraît favoriser ni défavoriser aucune portion de la population (à la différence du profilage ethnique par exemple). Cette atopie peut paraître providentielle, dans la mesure où elle semble permettre d'éviter l'aporie d'un savoir toujours situé (lié au fait que nous avons des corps, qui occupent une certaine place dans l'espace, qui ne nous permettent donc qu'un certain point de vue sur les choses), mais elle rend aussi ce « savoir » algorithmique inappropriable pour les êtres humains dans la mesure, justement, où il n'est pas situé. L'idée étant que le « savoir » ou la « vérité » ne seraient plus construits mais toujours déjà là, immanents aux banques de données, dans l'attente d'être mis au jour par des algorithmes réalisant des opérations statistiques sur ces masses de données y découvrent des ensembles de corrélations permettant de modéliser les comportements, attitudes, trajectoires et événements du monde plus finement au fur et à mesure que la quantité de données disponibles s'accroit.

Nous en oublierions presque ce que nous martèlent depuis les années 1970, les *Sciences and Technologies Studies* à travers les écrits de Bruno Latour, de Steve Woolgar, de John Law, de Sheila Jasanov notamment et, avant eux déjà, de Michel Foucault : à savoir que les « données » ne sont jamais « données », mais résultent toujours de processus de production (nos données d'identité elles-mêmes sont produites par l'État civil). Et les données du *Big Data* ne font pas exception[139] – seulement, leur quantité, leur complexité, la vitesse à laquelle elles sont produites et remplacées par d'autres ne ménagent plus vraiment ni l'espace, ni le temps de la critique, des épreuves de validation, de véridiction. On se débrouille autrement : l'opérationnalité en « temps réel », la fiabilité sans vérité des «modèles » produits algorithmiquement, leur très grande plasticité (apprenant de leurs « erreurs », ils s'affinent en temps réel) compensent pragmatiquement les incertitudes de leur statut épistémologique.

À la *passion de l'épreuve*[140], de la mise à l'épreuve du monde, des autres et de soi semble dès lors succéder une passion pour le réel immédiat – non plus le réalisme ni la justesse, ni l'élégance de la représentation, mais le réel comme tel - sans médiation, remisant au rang des gesticulations et fantasmes inutiles les actes d'énonciation, de transcription, de qualification, d'évaluation : « *Data is enough* », les données parlent d'elles-mêmes. À l'ubiquitaire crise de la représentation

137. I. Ayres, *Super Crunchers : Why thinking by numbers is the new way to be smart*, Bantam, Août 2008. Voir aussi A. Pentland, *Social Physics, How Good Ideas Spread*. *The Lessons from a New Science*, Penguin Press, 2014.

138. C. Anderson, « The End of Theory : The Data Deluge Makes the Scientific Method Obsolete", *Wired Magazine*, 23 juin 2008.

139. I. Bastard, D. Cardon, G. Fouetillou, C. Prieur, S. Raux, « Travail et travailleurs de la donnée », InternetActu, http://www.internetactu.net/2013/12/13/travail-et-travailleurs-de-la-donnee/

140. A. Ronell, *Test Drive. La passion de l'épreuve*, Stock, 2009.

(politique, artistique, scientifique…) l'idéologie des *Big Data* apporte une réponse radicale : nous n'avons plus rien à re-présenter, le « numérique » instaurant un régime d'actualité pure, absorbant dans le vortex du temps réel à la fois le passé et l'avenir, encore et déjà disponibles, sous forme latente, à même les jeux de données. Nous n'aurions plus à faire rapport de nos activités, le rapport étant simultané à l'activité, cette dernière produisant d'elle-même les données qui servent à affiner le profil de performance, y compris les projections de nos performances futures, en temps réel.

5. Résister aux sirènes de l'objectivité numérique au nom de la justice comme processus et horizon inclôturables

Le caractère ubiquitaire, prétendument total, et en tous cas peu sélectif de la numérisation du monde, et l'objectivité mécanique de la constitution algorithmique des profils, en cela démocratique et égalitaire qu'ils visent tout le monde sans plus viser personne en particulier, tout cela fait de la catégorisation algorithmique un phénomène indépendant des systèmes de différenciations juridiques ou traditionnelles (en fonction du statut, de privilèges, d'avantages ou désavantages socio-économiques…) identifiés par Boltanski et Thévenot comme ce sur quoi s'appuie un modèle de cité qui en justifie ou en légitime les « états de grandeur » et dont l'existence est à la fois une condition et un effet des relations de pouvoir[141]. Si cette utopie d'un accès immédiat au réel *comme tel*, à travers son « double » numérisé, et d'une modélisation du monde social à même le monde numérisé lui-même[142], transcendant toutes les formes instituées, a de quoi séduire le monde juridique, elle a aussi de quoi « vider le juridisme de ses appuis classiques » (la causalité, la succession temporelle, le sujet capable d'entendement et de volonté…), et faire passer la « gouvernementalité algorithmique »[143] pour une alternative (plus opérationnelle, moins coûteuse…)[144] à l'État de droit et aux lourdeurs et incertitudes de ses scènes administrative, législative et judiciaire[145].

La cécité du *datamining* relativement aux catégorisations socialement éprouvées, et discriminantes, son impartialité donc, serait, de l'avis de Tal Zarsky, l'une des mauvaises raisons pour lesquelles le *datamining* serait si mal perçu par la majorité. Zarsky présuppose qu'en général les individus relevant de « la majorité »

141. L. Boltanski et L. Thévenot, *De la justification. Les économies de la grandeur*, Gallimard, 1991, p.162.

142. I. Ayres, *Super Crunchers : why Thinking By Numbers is the new way to be smart,* Bantam; Reprint edition (August 26, 2008).

143. Sur la notion de gouvernementalité algorithmique, nous nous permettons de renvoyer le lecteur à A. Rouvroy, T. Berns, "Gouvernementalité algorithmique et perspectives d'émancipation. Le disparate comme condition d'individuation par la relation", *Réseaux*, *Politiques des algorithmes. Les métriques du web*, N. 117, 2013/1, pp. 163-196.

144. R. Calo, « Code, Nudge, or Notice ?», *Iowa Law Review*, 2014, vol.99, no.2, pp. 773-802.

145. A. Rouvroy, "Pour une défense de l'éprouvante inopérationnalité du droit face à l'opérationnalité sans épreuve du comportementalisme numérique", *Dissensus. Revue de Philosophie politique de l'Université de Liège*, 2011, n.4. http://popups.ulg.ac.be/2031-4981/index.php?id=1269&file=1&pid=963.

préfèrent que la charge (en termes de coûts et d'inconvénients) des phénomènes de surveillance soit focalisée sur des groupes minoritaires spécifiques dépourvus de relais politiques plutôt que de subir eux aussi un système de surveillance qui y soumettrait tout le monde de manière égalitaire (sous une sorte de « voile d'ignorance »). L'hypothèse est bien sûr d'autant plus plausible que nous nous trouvons pris dans des formes d'organisation sociale dont l'on sait qu'elles favorisent les comportements concurrentiels et sanctionnent les comportements solidaires. Zarsky soutient donc que les réticences du public relativement à l'idée de substituer le datamining aux opérations humaines de détection et d'évaluation, inévitablement biaisées en défaveur des minorités les moins favorisées, relèvent de la tyrannie de la majorité[146]. C'est bien, une fois encore, l'objectivité et l'impartialité des processus algorithmiques hyper-vigilants mais plus aveugles que la justice, Thémis aux yeux bandés, qui se trouvent ainsi célébrées. « Etre objectif, c'est aspirer à un savoir qui ne garde aucune trace de celui qui sait, un savoir vierge, débarrassé des préjugés et des acquis, des fantasmes et des jugements, des attentes et des efforts. L'objectivité est une vision aveugle, un regard sans inférence, sans interprétation, sans intelligence. »[147]

Mais sans doute faudrait-il problématiser davantage le rapport entre objectivité et justice. Les arguments fondés sur l'objectivité (ontologique, mécanique ou a-perspective[148]), ne sont-ils pas plutôt des injonctions d'obéissance aveugle, d'exclusion de toute forme de critique ou de problématisation, que l'ouverture d'une évaluation équitable, juste, des personnes et des situations ? Que penser d'une objectivité qui dispense de la critique, de la discussion, de la mise en procès ?

Par ailleurs, les opérations de *datamining* et de profilage n'apparaissent objectives et égalitaires que dans la mesure où l'on ignore qu'elles sont aveugles et sourdes à tout ce qui, du monde – les idiosyncrasies individuelles, les raisons des actions - ne se laisse pas traduire sous une forme numérique. Dès lors que l'on prend acte de leurs angles morts, il devient possible de comprendre en quoi ces catégorisations automatiques et « objectives », en ce qu'elles construisent une « réalité » en présupposant toutes choses égales par ailleurs, peuvent n'être pas « justes » sans pour autant cesser d'être objectives et impartiales. Pourtant, le propre du comportementalisme numérique est que son objectivité semble le dispenser de toute opération de justification, si par justification l'on entend « l'activité qui consiste à chercher les raisons d'une action ou des raisons pour soutenir une décision, une opinion ou autre expression symbolique, sur le motif qu'elle est juste ou raisonnable. »[149]

---

146. T. Zarsky, "Governmental Data Mining and its Alternatives", 2011, *Penn State Law Review*, Vol. 116, No. 2: "*if data mining is accepted by the legislature, it might only require limited judicial review. This is as opposed to the use of profiles and field officer discretion, which calls for greater scrutiny*."

147. L. Daston et P. Galison, *Objectivité*, traduit par Sophie Renaut et Hélène Quiniou, Les presses du réel, 2012, p.25.

148. L. Daston, "Objectivity and the escape from perspective", *Social Studies of Science*, Vol. 22, 1992, p. 597-618.

149. J. Wroblewski, "Définition de la justification", *Dictionnaire encyclopédique de théorie et de sociologie du droit*, A.-J. Arnaud (dir.), Paris, LGDJ, 2ème édition, 1993, p.332.

En d'autres termes, si le *datamining* peut effectivement se présenter comme un rempart contre la tyrannie de la majorité, les catégories qu'il produit ne sont pas nécessairement « justes » ni « équitables ». Elles le seraient si, par exemple, les notions de justice actuarielle (en fonction de laquelle toute distinction de traitement économiquement justifiée est actuariellement juste) et de justice sociale se recouvraient parfaitement, ce qui n'est bien évidemment pas le cas. Une distinction de traitement qui exclurait par exemple systématiquement les personnes victimes de violences conjugales du bénéfice de l'assurance vie, quel que soit le sexe, l'origine sociale de ces personnes, sur base d'une attribution de profil de risque établi par une méthode inductive de *datamining*, pourrait bien être algorithmiquement et économiquement « rationnelle », actuariellement justifiée, et socialement injuste. On perçoit bien, en l'occurrence, le danger associé au déploiement d'un régime de vérité numérique impartiale et opérationnelle mais qui dispenserait de toute discussion politique, de toute décision collective, et de toute contestation relative aux critères de besoin, de mérite, de dangerosité, de capacités qui président aux catégorisations bureaucratique et/ou sécuritaire des individus et comportements. Dans la pratique du droit, la justice est un processus de construction continue qui présuppose et organise les possibilités de contestation de ses propres productions.

Imaginons même que les processus de profilage deviennent extrêmement fins, précis, et qu'ils permettent de tenir compte en temps réel des variations les plus infimes dans les comportements individuels, et désarment l'objection souvent opposée aux statistiques « traditionnelles » : le fait qu'elles négligent nécessairement toute une série de facteurs et ne donnent de la réalité sociale qu'une vision biaisée par l'inévitable sélectivité des bases statistiques. Eh bien, quand bien même le bouquet de profils entourerait chaque personne d'une aura prédictive aussi bien ajustée qu'une seconde peau, il ne serait pas encore justifié de se passer de l'évaluation humaine et de la rencontre, car, précisément, l'objectivité « absolue » pour peu qu'elle existe un jour, serait incompatible avec l'idée d'une justice qui reste un horizon inatteignable et, parce qu'elle reste inatteignable, justifie la prudence du juge, le doute, le scepticisme, cela même qui conserve à la norme juridique une vivante plasticité[150].

La proposition de Règlement du Parlement européen et du Conseil relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (règlement général sur la protection des données)[151] confirme d'ailleurs, en son article 20 – reprenant et

150. À cet égard voir J. Derrida dans *Force de Loi : Les fondements mystiques de l'autorité,* Galilée, 1994, paru précédemment en Anglais sous le titre « The force of law », in Deconstruction and the Possibility of Justice, Cornell, D. Rosenfield, M. and Gray, D. (eds), Routledge, 1992.

151. COM(2012) 11 final. Les exceptions au principe sont autorisées lorsque la mesure fondée sur le profilage est effectuée dans le cadre de la conclusion ou de l'exécution d'un contrat, moyennant certaines conditions, ou est expressément autorisée par une législation de l'Union ou d'un État membre qui prévoit également des mesures appropriées garantissant la sauvegarde des intérêts légitimes de la personne concernée ; ou encore lorsqu'elle est fondée sur le consentement de la personne concernée, sous certaines conditions. Dans tous les cas,

complétant, pour tenir compte des nouvelles possibilités de profilage algorithmique, l'article 15 de la Directive 95/46/CE que la proposition de Règlement a vocation à remplacer – le principe suivant lequel :

«*Toute personne a le droit de ne pas être soumise à une mesure produisant des effets juridiques à son égard ou l'affectant de manière significative prise sur le seul fondement d'un traitement automatisé destiné à évaluer certains aspects personnels propres à cette personne physique ou à analyser ou prévoir en particulier le rendement professionnel de celle-ci, sa situation économique, sa localisation, son état de santé, ses préférences personnelles, sa fiabilité ou son comportement (…)* ».

Il nous semble que ce n'est pas tant le risque d'erreur de profilage qui justifie cette disposition que la considération suivant laquelle quand bien même les données traitées, individuellement, ne seraient à proprement parler des données à caractère personnel, il est néanmoins raisonnable de penser que les citoyens ont un intérêt légitime à ne pas voir des quantités substantielles d'informations à propos de leurs activités, trajectoires ou attitudes exploitées à des fins de profilage de leurs comportements par leurs gouvernements ou par des firmes privées[152].

6. La réalité augmentée du possible : clôture du réel numérisé

La question est donc celle-ci : comment, et au nom de quoi limiter la prolifération des données susceptibles de nourrir les profilages dont nous sommes les cibles ? Nous n'avons appris à nous méfier que des traitements automatisés de données à caractère personnel, or celles-ci n'interviennent que très marginalement dans les phénomènes qui nous intéressent ici. Cette fétichisation de la donnée personnelle – renforcée par le droit – nous fait passer à côté de ce qui fait aujourd'hui problème. Les formes de pouvoir qui s'exercent aujourd'hui sur les individus passent peut-être beaucoup moins par les traitements de données à caractère personnel et l'identification des individus que par des formes algorithmiques de catégorisations impersonnelles, évolutives en continu, des opportunités et des risques, c'est-à-dire des formes de vie (attitudes, trajectoires…). Un profil, ce n'est en réalité personne – personne n'y correspond totalement, et aucun profil ne vise qu'une seule personne, identifiée ou identifiable.

Pourtant, être profilé de telle ou telle manière, affecte les opportunités qui nous sont disponibles, et ainsi, l'espace de possibilités qui nous définit : non seulement ce que nous avons fait ou faisons, mais ce que nous aurions pu faire ou pourrions faire dans l'avenir[153]. Avec le profilage algorithmique, le pouvoir a changé de cible : pas le probable, mais le potentiel, la potentialité pure, la dimension de virtualité dans le réel. Ce qui est visé – ce que l'on veut, si ce n'est éradiquer, au moins neutraliser

---

lorsqu'une mesure est prise sur base du profilage automatique, les personnes concernées doivent être informées de l'existence de ce profilage, de la logique sous-tendant le traitement automatisé des données qui le concernent, et de ses effets escomptés pour sa personne.

152. À cet égard, lire notamment Gray, D. C. and Citron, D. K., « A Technology-Centered Approach to Quantitative Privacy », 14 août 2012. SSRN : http://ssrn.com/abstract=2129439.

153. À cet égard, voir I. Hacking, "Making Up People", *London Review of Books*, 2006, vol.26, no.16, pp. 23-26.

dans ses effets suspensifs/interruptifs des flux – c'est la dimension de puissance des individus : leur propension à ne pas être là où on les attend, à vouloir quelque chose qui n'aurait pas été prévu pour eux, leur capacité à se découvrir radicalement neuf, à se surprendre eux-mêmes en quelque sorte. Dimension événementielle par excellence, c'est cette dimension, virtuelle sur le plan individuel, et utopique sur le plan collectif, ce « reste » inactualisable[154], qui est directement affecté et intentionnellement visée par les industriels du marketing, les professionnels de la sécurité, de la lutte anti-terroriste, ou encore de la prévention des fraudes. Le « succès » de la « raison algorithmique » – qui est aussi une déraison (si l'on considère la manière assez radicale dont l'induction statistique s'écarte des ambitions de la rationalité « moderne » qui visait à comprendre et prédire les phénomènes en les reliant à leurs causes) – est proportionnel à sa capacité à aider les bureaucraties tant privées que publiques à *anticiper*, à défaut de pouvoir les *prévoir*, les potentialités et virtualités dont les individus et les situations sont porteurs, c'est-à-dire à percevoir anticipativement ce qui n'est pas (encore) manifeste tout en dispensant du « travail » ou de l'effort, coûteux en temps et en argent, d'éprouver, tester, expérimenter, interroger le monde physique pour lui faire « dire » les puissances, possibilités, potentialités qu'il recèle. Nul besoin d'encore s'en remettre au témoignage, à l'aveu, à la confession, au discours d'expert ou d'autorité, ou au récit d'expérience. Nul besoin, non plus, pour anticiper ce qui peut advenir, de s'attacher à identifier les causes des phénomènes, ou encore les intentions des individus. L'induction algorithmique dispense de tout effort herméneutique, mais aussi de toute comparution des individus ou des objets « en personne », de toute communauté donc.

On pourrait croire que tout ceci n'est que science fiction. Il n'en est rien. Si l'on en croit Eric Schmidt, directeur chez Google, bientôt la technologie deviendra tellement efficace qu'il sera très difficile pour les personnes de voir ou consommer quelque chose qui n'aura pas été prévu pour eux[155]. Bien sûr, dans le domaine du marketing, l'objectif n'est pas tant d'adapter l'offre aux désirs spontanés (pour peu qu'une telle chose existe) des individus mais plutôt d'adapter les désirs des individus à l'offre, en ajustant les stratégies de vente (le moment de l'envoi de la publicité, la manière de présenter le produit, d'en fixer le prix…), le design de l'interface (de manière à susciter la confiance et l'envie de consommer) au profil

154. « *Dans le rapport qu'une époque entretient avec elle-même, il y a toujours d'un côté ce qu'elle consomme et consume, et de l'autre ce reste, cet inachevé qui est très difficile à déterminer mais qu'on pourrait définir comme ce qu'elle n'a pas réalisé, ce à quoi elle a seulement pensé ou rêvé, et qui s'est déposé dans les œuvres, en tout cas dans certaines œuvres, mais aussi dans les paysages, les outils, les chants. Chaque époque dépose ainsi une couche qui reste en dormance pour plus tard. Et c'est alors qu'il faut être historien. L'historien, comme disait Benjamin, c'est celui qui convoque les morts au banquet des vivants. Et en particulier pour témoigner que ce à quoi ils avaient pensé n'est pas venu mais n'a pas disparu non plus, continue d'être là, est en latence et, d'une certaine manière, résiste. En ce sens, l'histoire est toujours un retour, mais qui est là pour réveiller cette formidable latence du passé et avec elle produire l'innovation. » (*J.-C. Bailly, « Tout passe, rien ne disparaît », *Vacarme,* n.50, 21 janvier 2010*.)*

155. http://online.wsj.com/news/articles/SB10001424052748704901104575423294099527212

de chacun.[156]La librairie en ligne *Amazon* brevetait récemment un logiciel lui permettant d'envoyer les marchandises vers ses clients avant même que ceux-ci n'aient procédé à l'acte d'achat[157]. Les centres d'appel téléphoniques de certaines entreprises, plutôt que d'évaluer les candidats sur la base du *curriculum vitae* et d'un entretien d'embauche, ont recours à des systèmes de sélection automatisés qui détectent, parmi toutes les informations disponibles sur les réseaux sociaux notamment, non pas directement si le candidat possède les qualités requises mais s'il correspond à certains points de données a priori sans rapport causal (comme le fait d'être inscrit sur deux réseaux sociaux plutôt que sur trois ou sur un seul) mais statistiquement prédictifs d'une bonne performance pour le poste vacant…[158]

La cible délibérée du gouvernement par les algorithmes est cette part d'incertitude radicale à laquelle la liberté individuelle est adossée, et qui en fait un événement jamais totalement actualisé, et donc toujours susceptible de développements imprévus.

L'incertitude radicale – que les nouvelles pratiques d'anticipation et de préemption s'efforcent de court-circuiter ou de neutraliser – est évidemment coûteuse. Ce coût, dans la société actuarielle, était pris en charge par des formes diverses de mutualisation du risque. Dans bien des domaines, la mutualisation des risques tend à faire place à une approche tentant de déterminer pour chacun ses « coûts réels » - une manière d'individualiser le risque et, du même coup, de détricoter les mécanismes de solidarité devant ce que l'on appelait autrefois « la providence ». Dans la société actuarielle, l'on se satisfaisait de dompter l'aléa en calculant les probabilités et en en répartissant la charge : cette répartition étant une manière de rendre supportable un reste incompressible d'incertitude radicale, l'excès du possible sur le probable. C'est précisément pour neutraliser ce *reste* que fleurissent aujourd'hui les politiques préemptives consistant à faire, anticipativement comme si l'événement redouté avait eu lieu et à prendre immédiatement les mesures s'imposant en conséquence (refus d'assurance à un fraudeur potentiel, élimination préventive d'un terroriste potentiel, orientation professionalisante des enfants sur base d'un profilage précoce…).

La notion de « nominalisme dynamique » développée par Ian Hacking est à cet égard particulièrement pertinente pour décrire l'effet performatif des classifications ou profilages réalisées sur base de corrélations statistiques : lorsque les individus font ainsi l'objet de catégorisations scientifiques ou bureaucratiques, quelles qu'en soient les finalités (contrôle, surveillance, assistance, orientation scolaire ou professionnelle, organisation, marketing…), ces catégorisations elles-mêmes affectent les personnes dans leurs comportements, ce qui a pour effet, en retour, d'affecter la classification[63].

156. À ce sujet, voir R. Calo, "Digital Market Manipulation", *George Washington Law Review*, 82, 2014.

157. G. Bensinger, "Amazon Wants to Ship Your Package Before You Buy It », *The Wall Street Journal*, 17 janvier 2014. http://blogs.wsj.com/digits/2014/01/17/amazon-wants-to-ship-your-package-before-you-buy-it/

158. H. Guillaud, "L'emploi à l'épreuve des algorithmes", *InternetActu*, 3 mai 2013, http://www.internetactu.net/2013/05/03/lemploi-a-lepreuve-des-algorithmes/

Cette clôture du numérique sur lui-même instaure une sorte de métabolisme normatif tout à fait étranger au métabolisme juridique dans lequel l'irréductibilité ou la non-coïncidence, ou l'excès de la personne, dans sa singularité, relativement aux faits qui lui sont reprochés (si l'on prend l'exemple du procès pénal), est à la fois ce qui oblige à parler et ce qui constitue cette part inconnue d'incertitude radicale, ou l'excès du possible sur le probable, qui a toujours constitué une provocation pour les institutions (dont les institutions législatives et judiciaires), de même que ce que l'on appelle communément la liberté, a toujours constitué une provocation pour les formes instituées de pouvoir, provocation salutaire dans la mesure où, tenant le monde et ses représentations à distance l'un de l'autre, la liberté humaine, et, plus généralement, la couteuse incertitude à laquelle et dont elle participe[159], étant précisément ce qui rend nécessaires les représentations institutionnelles et langagières, ouvre également la possibilité de la contradiction herméneutique[160] et de la critique, « une pratique qui suspend le jugement et une occasion pour de nouvelles pratiques de valeurs fondée précisément sur cette suspension»[161].

Dans son assaut de la « part inconnue d'incertitude radicale », et donc en vue d'amenuiser ou d'annihiler la distance entre la personne et la somme de ses profils, de plus en plus nombreux, de plus en plus précis, la nouvelle rationalité algorithmique, faisant l'économie de toute institutionnalisation, et donc de toute transcription, érode la logique de la représentation, et donc aussi les relations, échanges et symbolisations constitutives du commun[162].

159. Pour R. Musil, ce n'était pas la liberté humaine (en tant que *libre-arbitre*, et donc *autorité sur/de soi-même*), qui était source d'incertitude mais, bien plus profondément, le hasard, lui-même condition de possibilité des régularités observées. Dans cette perspective, c'est donc le hasard, et non la liberté, qui se présente comme arrière-fond nécessaire : « *Dans la vie ordinaire, nous n'agissons pas suivant une motivation, mais selon la nécessité, dans un enchaînement de causes et d'effets ; il est vrai qu'une part de nous-mêmes intervient dans cet enchaînement, nous permettant de nous juger libres. Cette liberté de la volonté est le pouvoir qu'a l'homme de faire volontairement ce qu'il veut involontairement. La motivation, elle, n'a aucun contact avec la volonté ; on ne peut la soumettre à l'opposition de la contrainte et de la liberté, elle est l'extrême contrainte profonde et l'extrême liberté. (…) Ce qu'on appelle encore aujourd'hui un destin personnel est évincé par les événements d'ordre collectif qui relevant de la statistique.* » (R. Musil, *Der Mann ohne Eigenschaften*, in. *Gesammelte Werke*, Rowohlt Verlag, 1978, p. 608, cité par J. Bouveresse, *Robert Musil. L'homme probable, le hasard, la moyenne et l'escargot de l'histoire*, L'éclat, 1993, p. 102-103).

160. Ce dont il s'agit, c'est de "*voir à l'intérieur de la vue*", selon la formule de Max Ernst, ou de regarder comme on voit.

161. M. Foucault, "Qu'est-ce que la critique ?", Compte rendu de la séance du 27 mai 1978, *Bulletin de la Société française de Philosophie*, avril-juin 1990. Il faut bien comprendre que la gouvernementalité algorithmique n'affecte pas tant les modalités du jugement - la manière suivant laquelle la réalité sociale se trouve subsumée dans des catégories préconstituées - qu'elle n'affecte, plus fondamentalement, les modalités de la critique – la manière dont sont produites les catégories à travers lesquelles le monde est appréhendé.

162. P. Legendre, *De la société comme texte. Linéaments d'une anthropologie dogmatique*, Fayard, 2001.

Quatre thèses sur la surveillance numérique de masse et la négociation de la vie privée

Par ***Antonio Casilli****,*
maître de conférences à Télécom ParisTech, chercheur en sociologie
au Centre Edgar Morin, École des hautes études en sciences sociales

Le débat politique actuel est agité par une inquiétude grandissante autour du déploiement de dispositifs numériques de surveillance généralisée qui s'appuient sur la collecte, le stockage et le traitement massif de données issues de transactions, échanges et usages quotidiens de technologies de l'information et de la communication. À partir des premières révélations d'Edward Snowden sur le programme états-unien PRISM, le grand public a appréhendé avec surprise et effroi l'étendue des interceptions auxquelles les services de renseignement des régimes démocratiques occidentaux ont soumis leurs propres citoyens. Ces événements sont en passe de modifier profondément le rapport gouvernants / gouvernés, contribuant à un climat d'instabilité géopolitique sans précédents, aggravé par le déclin du rôle des marchés comme tiers correcteurs des dérives sécuritaires des États. Au fur et à mesure que se précisent les responsabilités des acteurs de l'économie numérique dans la mise en place d'un vaste complexe militaro-industriel, s'amorce une phase de tension et de méfiance dans les rapports entre consommateurs et entreprises du secteur privé.

Dans l'espace où se déploient les enjeux politiques du numérique, des intérêts économiques et stratégiques promeuvent ces méthodes de surveillance, en prétendant s'inscrire dans la continuité des outils de contrôle des populations adoptés depuis longtemps par les États modernes. De fait, on ne pourrait pas vivre une rupture plus totale.

La mise en place d'un système de surveillance numérique de masse est rendue possible par la tendance sur le long cours à l'expression d'un exécutif fort, conjuguée avec la pénétration des logiques militaires dans l'appareil démocratique, voire par l'assimilation progressive entre enjeux de sécurité intérieure et doctrine de la sécurité nationale[163]. Si la tendance du pouvoir exécutif à s'exercer sans contrepoids peut être lue comme le propre d'un projet démocratique toujours *in fieri* (une « *démocratie inachevée* », selon Pierre Rosanvallon[164]), le phénomène sécuritaire se distingue par sa capacité à s'ériger en discours ambiant qui conditionne les

163. G. Périès, *Les dilemmes européens de la gestion des identités numériques : entre la confiance et la sécurité nationale*, conférence Chaire Valeurs Politiques et Informations Personnelles, Institut Mines-Télécom, 17 septembre 2013, http://cvpip.wp.mines-telecom.fr/2013/09/17/deuxieme-rencontre-de-la-chaire-le-mardi-17-septembre-2013-de-17h-a-19h-a-linstitut-mines-telecom/

164. P. Rosanvallon, *La démocratie inachevée. Histoire de la souveraineté du peuple en France*, Paris, Gallimard, 2000.

modes de la délibération démocratique, en obstruant d'un côté la capacité de contrôle par les pouvoirs législatif et judiciaire sur les organes exécutifs, et de l'autre les manifestations de la volonté générale de respect des libertés et des garanties fondamentales des citoyens.

1e thèse : la surveillance est devenue participative

Le débat actuel sur la protection de la vie privée est prisonnier d'une fausse dichotomie liberté / sécurité. Cette opposition est fonctionnelle à la promotion d'une capture indiscriminée d'informations personnelles, envisagée comme seule garantie contre les menaces internes et externes qui pèsent sur nos sociétés. L'instrument principal de cette érosion de la prérogative citoyenne au respect de l'intimité et du secret, est l'expédient rhétorique de *la recherche d'un équilibre*, d'une juste proportion entre droit collectif à la sécurité et droits individuels à la confidentialité des informations. Mais, comme le rappelle le spécialiste de la protection des données Caspar Bowden dans une audition de 2014 devant la commission renseignement et sécurité du gouvernement britannique, « *l'équilibre est une métaphore trompeuse. En ligne de principe il ne désigne qu'une harmonie instable avec un seuil unique, situé sur une échelle linéaire* »[165]. La poursuite d'un arbitrage optimal repose sur une représentation de la vie privée et de la sécurité publique comme deux polarités d'un *continuum*. Or, ce *continuum* a été brisé par le changement de la nature même de la surveillance.

Par rapport au passé, le système actuel de surveillance numérique des populations a une particularité : *celle de ne pas être une surveillance directe mais participative*.[166] Par cette formule nous désignons une surveillance mutuelle et horizontale basée sur le dévoilement volontaire et agonistique des données personnelles par les utilisateurs eux-mêmes des services numériques, applications mobiles, plateformes Web. Elle s'accompagne d'une perte de contrôle sur les conditions d'usage des plateformes et services web sur lesquels les données personnelles sont sauvegardées et mises en circulation. La surveillance est participative dans la mesure où elle est mutuelle, passant par une généralisation des mécanismes de modération par le bas et d'application communautaire de normes en vigueur sur les plateformes sociales.

Un passage symbolique s'opère alors, d'une surveillance basée sur un modèle de *Big Brother* vers une surveillance qui passerait par un *Big Other*, un Autre majuscule, incarnation d'une écrasante injonction sociale à la connectivité en temps réel. Sans ce présupposé, des programmes de surveillance basés sur l'accès direct aux grandes fermes de données n'auraient pas été concevables : la structure de surveillance est constamment nourrie par les objets mêmes de cette surveillance, inscrits dans un système social qui prime la participation basée sur le dévoilement réciproque finalisé à la construction de capital social en ligne.

---

165. C. Bowden, "Privacy and Security Inquiry: Submission to the Intelligence And Security Committee of Parliament", ISC, Londres, 7 février 2014, http://blog.privacystrategy.eu/public/published/ Submission_ISC_7.2.2014_-_Caspar_Bowden.pdf

166. A. Albrechtslund, Online Social Networking as Participatory Surveillance. *First Monday,* 13 (3), 2008, http://firstmonday.org/ojs/index.php/fm/article/view/2142.

Les citoyens connectés ne sont pas de simples objets passifs et la surveillance participative n'écrase pas leur volonté, mais au contraire la sollicite, la charge de la responsabilité même de conduire les opérations nécessaires à sa mise en œuvre, ainsi que de trier, selon le contexte, la temporalité et la quantité de données à dévoiler. *Dans la mesure où cette quantité est déterminée par des critères régissant une sociabilité quotidienne, et non pas par la nécessité de préserver la sécurité des citoyens, la recherche d'un équilibre ou d'une juste proportion entre les deux s'avère illusoire.*

Il ne faut pas voir dans le fait que les citoyens concourent aux usages de ces plateformes sociales un signal d'illettrisme ou d'adhésion idéologique, mais au contraire celui d'une capture de leurs flux de communications par une architecture de la participation passant par la production de traces qui personnalisent les usages, documentent les passages et la présence dans les environnements numériques[167]. L'ordre de priorités entre protection de la *privacy* et personnalisation de l'expérience numérique semble être alors inversé, face à ces traces dont la pérennité et les utilisations secondaires (autant à des fins commerciales que sécuritaires) échappent aux utilisateurs.

2e thèse : les annonces de « la fin de la vie privée » sont erronées et idéologiquement biaisées

La question de la vie privée – inéluctablement, douloureusement au centre du débat politique et citoyen des dernières années – révèle les limites d'une posture théorique qui a dominé les médias et le débat public pendant longtemps, convergeant sur l'annonce de « fin de la *privacy* », de sa disparition de l'horizon de nos pratiques quotidiennes et de nos préoccupations politiques, prélude de son abrogation de nos dispositifs juridiques.

Cette hypothèse a été principalement portée par les grands intérêts industriels, notamment les géants du secteur numérique. Une ligne imaginaire unit la conférence de presse de 1999 où le PDG de Sun Microsystems, Scott McNealy, décrétait « *De toute façon vous avez zéro vie privée. Tournez la page !* »[168] à la réunion de la *Federal Trade Commission* de 2013 où le mathématicien Vinton Cerf, en sa qualité d'« évangéliste en chef » de Google, affirmait que d'un point de vue historique « *la vie privée pourrait très bien être une anomalie* »[169]. Cette perspective prend son sens dans un récit fortement stylisé et politiquement orienté de la transition à la modernité, selon lequel nos sociétés seraient passées d'une structure sociale caractérisée par des petites communautés locales, où chaque individu avait connaissance de l'ensemble des actions et des opinions de ses voisins et proches, à une société urbaine avec l'idée d'une sphère d'action et de pensée privée imposée par la bourgeoisie naissante ; aujourd'hui, la parenthèse

167. L. Merzeau, «L'intelligence des traces», *Intellectica,* 2013, 59(1) : 115-135.

168. P. Sprenger, "Sun on Privacy : 'Get Over It'", *Wired*, 26 janvier 1999, http://archive.wired.com/politics/law/news/1999/01/17538.

169. G. Ferenstein, *Google's Cerf Says "Privacy May Be An Anomaly". Historically, He's Right.,* TechCrunch, 2013, consulté le 22 juin 2014, http://techcrunch.com/2013/11/20/googles-cerf-says-privacy-may-be-an-anomaly-historically-hes-right/.

historique de la vie privée serait prétendument en train de se refermer, dans une évolution inévitable et spontanée des comportements sociaux des utilisateurs des réseaux sociaux numériques. La « nouvelle norme » (pour reprendre la définition donnée par Mark Zuckerberg en 2010)[170] serait la transparence, la vie en public. Ce changement serait inscrit dans la longue durée de l'histoire. Il légitime, en les intégrant à une grande dynamique collective, les offres de services de connectivité basés sur l'extraction de données personnelles des consommateurs. Les porte-parole des géants du Web n'ambitionnent rien de moins que de montrer qu'ils visent à mettre fin à l'existence isolée et aliénée des grandes villes industrielles des siècles derniers. Revenir en arrière, dans un effort de restauration historique et culturelle, à une époque qu'ils dépeignent comme un temps d'harmonie et de transparence des cercles de sociabilité primaire, serait un effet de leur effort de construire un monde interconnecté.

D'autres acteurs, aussi bien savants que représentants de la société civile, adhèrent eux aussi au discours de la fin de la vie privée en décrivant comme paradoxales et alarmantes les postures des individus en réseau[171]. Les utilisateurs de services du web social et des dispositifs mobiles accepteraient de renoncer progressivement à leur vie privée pour bénéficier d'avantages commerciaux. Les usages évolueraient vers plus de transparence, dans un régime de partage généralisé où le traçage de la part des pouvoirs publics et des entreprises privées irait de pair. Quoique inspirés de motivations théoriques et politiques bien différentes des acteurs industriels, les partisans de cette approche issus de la société civile et du monde intellectuel aboutissent à la même prédiction des acteurs du numérique qu'ils cherchent à contrer : la vie privée aurait bel et bien disparu.

Pourtant les comportements constatés vont à l'encontre de cette prédiction. À ce climat idéologiquement chargé, les utilisateurs opposent de manière de plus en plus pressante une exigence d'autonomie et de capacitation personnelle et collective. Face à l'étendue des complicités entre entreprises et États, au scandale des lois sécuritaires, au manque de moyens légaux et techniques de protection de l'intégrité et de la confidentialité des informations personnelles, les usagers ne restent pas passifs. Affirmer ce dernier point, comme certains commentateurs peu avertis le font, est fallacieux. La perte de confiance des usagers va de pair avec une demande importante de services de sécurisation et d'anonymisation des échanges[172]. La généralisation des usages de réseaux cryptographiés comme TOR, de systèmes d'exploitation « amnésiques » comme Tails, de sites web et d'applications « éphémères », sont autant d'indications claires d'une demande croissante d'outils permettant la maîtrise de sa présence numérique.

---

170. «The Zuckerberg Files, Facebook CEO Mark Zuckerberg : TechCrunch Interview At The Crunchies", Transcript, 8 janvier 2010, http://dc.uwm.edu/zuckerberg_files_transcripts/32/.

171. P. A. Norberg, Daniel R. Horne et David A. Horne, "The Privacy Paradox: Personal Information Disclosure Intentions versus Behaviors ». *Journal of Consumer Affairs*, 41, 1 : 100-126. doi:10.1111/j.1745-6606.2006.00070.x, 2007.

172. L. Rainie, S. Kiesler, R. Kang et M. Madden, « Anonymity, Privacy, and Security Online », *Pew Research Center's Internet & American Life Project*, consulté le 18 juin 2014, http://www.pewinternet.org/2013/09/05/anonymity-privacy-and-security-online/.

Les grandes entreprises du web elles-mêmes ont réagi en proposant des services « concurrentiels en termes de vie privée » (par exemple la démocratisation du cryptage du courrier électronique dans Gmail) ou en rachetant au prix fort des entreprises qui minimisent la collecte de métadonnées (v. les 19 milliards de dollars déboursés par *Facebook* pour *WhatsApp* en 2014). En revanche, d'autres secteurs du numérique subissent le contrecoup de ces nouvelles sensibilités culturelles et politiques. C'est le cas des entreprises du *cloud* qui encourent des pertes estimées, rien que pour les États-Unis, jusqu'à 35 milliards de dollars sur trois ans[173].

Qu'elle soit motivée par des intérêts commerciaux ou par des enjeux politiques, la restitution historique sous-jacente à l'hypothèse de la fin de la vie privée reste en conséquence sujette à controverse. Plutôt qu'une transition pacifique et linéaire d'un monde où la *privacy* aurait joué un rôle significatif à un monde où elle aurait perdu sa raison d'être, nous vivons aujourd'hui une véritable guerre culturelle autour de la vie privée. Rien ne garantit que cette guerre sera gagnée par les États ou les propriétaires des grandes exploitations de données qui entretiennent le régime actuel de surveillance participative de masse. Il nous faut aujourd'hui plus que jamais sortir du cadre idéologique dans lequel nous sommes enfermés, celui de la vie privée comme circonstance historique fortuite, pour reconnaître qu'elle est un enjeu qui, loin de faiblir, se généralise dans une société en réseau.

3e thèse : au lieu de s'estomper, le souci de la vie privée se démocratise dans la société en réseau

Contrairement à l'idée reçue de la disparition de la vie privée, l'importance accordée à la gestion des limites et des contenus de la sphère personnelle des citoyens s'amplifie dans le contexte social et technologique actuel. En cohérence avec la lecture qu'offrait Michel Foucault du « souci de soi »[174], le *souci de la vie privée* peut être décrit comme un travail de définition de la frontière entre public et privé, à savoir entre responsabilités et contraintes collectives et ce qui relève de la capacité individuelle de penser et d'agir.

Pour sortir du cadre idéologique actuel, il faut recontextualiser les origines historiques de la notion de vie privée. La situation de départ, pour reprendre la reconstruction que fait Philippe Ariès de ce processus, est marquée par une vie sociale ni privée ni publique au sens que nous accordons aujourd'hui à ces termes. Avant l'époque moderne, les interactions dans l'espace commun dessinent encore un espace indistinct où l'intimité individuelle est dissipée dans le tissage des

173. D. Castro, "How Much Will PRISM Cost the U.S. Cloud Computing Industry? ", *in Washington, DC : The Information Technology & Innovation Foundation*, 5 août 2013, http://www.itif.org/publications/how-much-will-prism-cost-us-cloud-computing-industry.

174. Cf. « *La tâche de s'éprouver, de s'examiner, de se contrôler dans une série d'exercices bien définis place la question de la vérité – de la vérité de ce que l'on est et de ce qu'on est capable de faire – au cœur de la constitution du sujet moral* », Michel Foucault, *Le Souci de soi*, Gallimard, Paris, 1984.

structures « *collectives, féodales et communautaires, à l'intérieur d'un système qui fonctionne à peu près : les solidarités de la communauté seigneuriale, les solidarités lignagères, les liens vassaliques* »[175].

Au fil des siècles, la rupture progressive des équilibres de pouvoir qui soutiennent ces structures fait surgir les spécificités de la sphère privée, non seulement comme possibilité abstraite, mais comme souci concret qui occupe et traverse les activités et les orientations des individus modernes. Ce souci est instrumenté par des dispositifs sociaux qui deviennent autant d'indices d'un changement des mentalités : *l'analyse de soi à travers l'écriture*, aidée par l'alphabétisation de masse et l'imprimerie ; les styles relationnels autonomes et égalitaires, avec l'accent mis sur *l'amitié* entre pairs ; la *re-spatialisation* des habitats, avec une préférence pour les logements particuliers par rapport aux endroits communs et aux maisons familiales. Toutes ces transformations peuvent être regardées comme l'écho de la « transformation de l'équilibre «nous-je» » à laquelle faisait référence Nobert Elias[176]. Significativement, l'Internet social des dernières années poursuit cette mouvance en intensifiant le recours à l'écriture de soi en ligne, au tissage de liens affinitaires d'amitié, et la re-spatialisation de l'expérience humaine – et généralise le souci de la vie privée, ainsi que l'exigence de sa protection.

L'apparition de la vie privée se situe entre la fin du Moyen Âge et le début de l'époque moderne. Cependant son apparition en tant que droit et prérogative à défendre est beaucoup plus récente. Le philosophe John Deigh[177] associe son émergence à la nécessité d'apporter une solution au problème de la « tyrannie de la majorité », initialement énoncé par Alexis de Tocqueville. La force redoutable de l'opinion publique et l'autorité du plus grand nombre dans les démocraties modernes mettent en danger l'autonomie des individus et des minorités. La nécessité de garantir la liberté intellectuelle et de statuer sur un ensemble de droits qui tempèrent le gouvernement sur les individus, conduit successivement le philosophe John Stuart Mill à formuler son « principe de non-nuisance ». Selon ce dernier la sphère privée est un contexte de liberté inviolable. « Le seul aspect », déclare Mill, « de la conduite d'un individu pour lequel il est redevable envers la société, est celui qui concerne les autres. Mais, pour ce qui ne concerne que lui, son indépendance est, de droit, absolue »[178].

C'est au sein de ce débat politique et philosophique que s'inscrit la réflexion sur la défense de la vie privée. Et c'est à cette tradition libérale que font référence Samuel Warren et Louis Brandeis, les deux juristes américains qui en 1890 consignent à la *Harvard Law Review* la définition désormais canonique du « droit à la vie privée » (*right to privacy*)[179]. En développant le « principe de non-nuisance » pour prendre

175. P. Ariès, «Pour une histoire de la vie privée», in Id., Georges Duby (dir.), *Histoire de la vie privée, t. 3 : De la Renaissance aux Lumières* (dir. Roger Chartier), Paris, Seuil, 1986.
176. N. Elias, *La société des individus*, Paris, Fayard, 1991.
177. J. Deigh, " Privacidad, democracia e internet ", *in* S. Champeau & D. Innerarity (dir.) *Internet y el Futuro de la Democracia*, Barcelona : Paidós, 2012.
178. J. S. Mill, «On Liberty», Londres : John W. Parker & Son, 1859, p. 22.
179. L. Warren et S. Brandeis, "The Right to Privacy", *Harvard Law Review*, 4(5), 1890.

en compte la nécessité de garantir non seulement la liberté d'action mais aussi la capacité même des individus de se soustraire au regard public, ils énoncent la *privacy* comme « le droit d'être laissé tranquille » (*right to be left alone*).

Comme le rappelle Deigh, cette innovation juridique est indissociable du contexte technologique et médiatique de la fin du XIXe siècle. Ce sont surtout la presse populaire, le photojournalisme et le journalisme d'enquête qui rendent nécessaire, dans la situation historique dans laquelle Warren et Brandeis écrivent, d'énoncer les contraintes de ce présupposé du fonctionnement public des démocraties modernes qu'est « une citoyenneté bien informée » (*a well-informed citizenry*).

Plus d'un siècle après cette première énonciation du droit à la *privacy*, la citoyenneté s'exerce par le biais de nouveaux médias. Il devient donc crucial d'interroger les effets des évolutions de l'écosystème médiatique et technologique pour reproblématiser la frontière entre privé et public. Dans une large mesure, les technologies sociales d'Internet prolongent les technologies des XIXe et XXe siècles de documentation et de capture d'images et d'autres contenus multimédias, attestant de comportements et d'opinions individuelles. Par ailleurs, elles généralisent le souci de la gestion et de la maîtrise de leurs effets. Prendre du recul d'un point de vue historique montre comment la prétendue nouvelle norme sociale de la transparence prônée par les acteurs industriels, et crainte par les utilisateurs, cache une réalité bien différente : la protection de la vie privée reste centrale, mais elle est soumise à une transformation qualitative qui entraîne un éloignement progressif de la tradition philosophique libérale anglo-saxonne et de son élaboration au sein de la jurisprudence du XIXe siècle. Si le photojournalisme d'enquête avait pu concerner un nombre limité de personnalités publiques et d'hommes politiques, le risque d'une capture inappropriée et de la diffusion d'éléments privés se généralise désormais à la société toute entière. Les petits et grands scandales de la vie privée des dernières années ne concernent plus uniquement les individus « de renom ». Le besoin de gérer ses traces, comme le montrent les difficultés d'application à grande échelle du « droit à l'oubli », se démocratise.

Cette histoire alternative de la notion de vie privée dépasse la simple hypothèse de la « fin de la *privacy* », ainsi que les visions négationnistes qui font de la vie privée une parenthèse historique, voire un événement nul et non avenu. Le souci de la vie privée est le produit de dynamiques culturelles, politiques et techno-médiatiques de longue haleine, qui se poursuivent dans la société en réseau. Il s'enchâsse dans des univers de pratiques et d'usages quotidiens et reflète la structuration de chacune des forces sociales en présence. Strictement lié au fonctionnement démocratique, il s'avère indissociable de l'élargissement progressif des libertés civiles et de leur généralisation auprès de couches de population de plus en plus importantes. Si historiquement l'exigence de la protection de la vie privée a été inégalement ressentie au sein des populations, c'est parce qu'elle est une préoccupation sensible aux hiérarchies et aux formes d'assujettissement propres aux diverses époques. Dans la mesure où les démocraties modernes prônent, du moins nominalement, un espace politique universellement accessible, le souci de la vie privée s'étend. C'est, comme le rappelait Hannah Arendt[180], la possibilité

180. H. Arendt, *The Human Condition*, Chicago : The University of Chicago Press, 1958.

même d'accéder à la vie active, professionnelle et publique, qui rend nécessaire une ligne de séparation entre ce qui relève de l'accomplissement collectif et ce qui est confiné au particulier à l'intime. Si cette possibilité était initialement circonscrite à une catégorie particulière d'individus, hommes libres et au revenu stable, elle s'élargit aujourd'hui à tous ceux (femmes, enfants, citoyens défavorisés…) dont l'exclusion de la vie publique rendait auparavant inutile de protéger la vie privée.

4e thèse : la vie privée a cessé d'être un droit individuel pour devenir une négociation collective

Les dernières décennies[181] ont conduit à une médiation technologique du droit à la vie publique et, en creux, à la vie privée. La vie citoyenne et l'expression de la volonté publique actuelle passent par l'usage de technologies de l'information et de la communication. Les usages numériques deviennent alors un *proxy* de la participation démocratique. Loin d'entraîner une érosion de la vie privée, ceci en fait une aspiration qui traverse la vie de tranches de plus en plus importantes de la population mondiale.

Mais le constat de cette généralisation du souci de la *privacy*, quoique important pour consolider le rejet de l'hypothèse de la « fin de la vie privée », n'équivaut pas à affirmer que rien n'a changé depuis l'essor du numérique. Nous choisissons d'indiquer la transition en cours par le passage d'une *privacy as penetration* à une *privacy as negotiation*.

La première approche se concrétise dans le « droit du particulier à être laissé tranquille » énoncé par Brandeis et Warren. Elle identifie un ensemble de données personnelles sensibles (les « *privacies of life* » dont parlait une célèbre sentence américaine de la même époque[182]) et les assoit au centre d'un espace individuel conçu comme un ensemble de sphères d'action concentriques. Ces données seraient, par leur essence même, « privées ». Telle vision renvoie à une hiérarchie rigide des informations, allant des plus personnelles et nécessitant une protection renforcée, aux moins sensibles, connues par un nombre toujours plus important d'acteurs sociaux. Il y aurait donc un noyau sensible à protéger, le reste pouvant être aisément rendu public, selon une vision nettement monodirectionnelle. Dans cette perspective, une invasion de la vie privée serait perpétrée par un agent extérieur qui parviendrait à pénétrer dans le noyau intime de la personne.

La *privacy* en tant que droit individuel, pour autant qu'elle incarne une attitude normative, représente une situation idéale, difficilement reconnaissable dans la vie courante. Elle devient un point de départ pour des élaborations successives, capables de prendre en compte les sensibilités nouvelles et les transformations technologiques. Dans un contexte de connectivité sociale médiatisée par les dispositifs numériques, la composition de la sphère intime de chaque individu ne

181. Les pages qui suivent reprennent et développent les propos contenus dans A. Casilli, « Contre l'hypothèse de la fin de la vie privée. La négociation de la privacy dans les médias sociaux », *Revue française des sciences de l'information et de la communication*, 3(1), 2013 http://rfsic.revues.org/630, consulté le 29 juin 2014.

182. *Boyd v. United States* (1886) 116 U.S. 616.

peut pas se réaliser dans l'isolement. Sur les plateformes sociales, personne n'a envie « d'être laissé tranquille », et pourtant tout le monde exprime un souci de *privacy* spécifique à sa personne. Dans les interactions courantes, les individus s'efforcent de contribuer activement au dévoilement ou au secret, à limiter les intrusions de l'extérieur et plus généralement à établir un jeu de règles et de privilèges d'accès à des aspects spécifiques de leur existence. En acceptant ou en évitant des interactions, en adaptant la fréquence et l'intensité des échanges, les individus mettent eux-mêmes en place des comportements explicitement ou implicitement finalisés à trier de manière dialectique et dynamique l'ensemble des informations susceptibles de faire l'objet d'interactions sociales.

Avec l'éclosion du Web, les acteurs sociaux sont davantage mis en condition de déployer une volonté stratégique de créer et entretenir leurs espaces d'autonomie. Dans ce nouveau paradigme, la *privacy* n'est pas une prérogative individuelle, mais une négociation collective. Elle résulte d'un aménagement relationnel, qui prend en compte des éléments intersubjectifs et se modèle selon les impulsions venant des personnes avec lesquelles un individu interagit. La spécificité de la vie privée dans le web social et des relations équipées par les technologies mobiles est un processus décentralisé, complexe et multidirectionnel. Le milieu social de chaque individu n'est pas donné a priori, mais au contraire se définit sous ses yeux. Cette circonstance, qui renvoie typiquement au cas d'un usager rejoignant une plateforme numérique de socialisation, impose avant tout d'évaluer le contexte d'interaction (ses participants, limites, codes, etc.) afin de pouvoir ajuster le contenu des communications. La construction de la présence en ligne d'un usager veut dire aussi bien se protéger contre les intrusions externes, que gérer les flux d'informations qu'il envoie lui-même vers l'extérieur. Pour ce faire, chaque individu procède normalement à un dévoilement progressif d'informations personnelles visant à solliciter des réactions de la part de la communauté de ses interacteurs.

À la différence du modèle classique de *privacy as penetration*, aucune de ces données partagées n'est privée, sensible ou intime en soi. Toute information est un signal envoyé par son auteur à son propre environnement, aux membres de son réseau personnel en ligne. Parce que ce signal vise à stimuler une réaction desdits membres, les individus s'entraident à adapter les informations qu'ils partagent en développant des postures d'écoute et de collaboration. Surtout, c'est après la collecte de ces *feedbacks* et évaluations, positives ou négatives, qu'ils établissent quelles informations doivent être considérées comme privées et lesquelles peuvent au contraire être dévoilées dans un contexte donné.

Parce qu'elle est basée sur la recherche d'un accord entre plusieurs parties, plus que sur une régulation émanant d'une seule d'entre elles, cette vision de la vie privée est assimilable à une négociation collective. Les acteurs recherchent une consonance, confrontent leurs intérêts, font des concessions mutuelles en termes de dévoilement et d'accès à des informations potentiellement sensibles. La perte de *privacy* sur certains éléments n'équivaut pas à une débâcle incontrôlée, mais plutôt à une retraite stratégique sur des sujets autour desquels la négociation est difficile. C'est par ce dévoilement collaboratif de soi accompagné de processus complexes de sélection et d'influence, que la surveillance participative est rendue

possible – ainsi que son dépassement. D'un point de vue citoyen, les programmes de surveillance de masse ne peuvent être contrés par l'affirmation d'un droit individuel à la vie privée comme une sphère qui résisterait à toute pénétration, mais en rétablissant un équilibre entre les forces en présence dans cette négociation : les États, les acteurs du marché, les individus.

Conclusion : contre la « privatisation de la *privacy* »

Définir la notion de vie privée en mettant l'accent sur les aspects de composition d'intérêts discordants de divers acteurs engendre, dans le contexte actuel, un réflexe que nous devons nous efforcer de contrer : celui qui pousserait à assimiler la « négociation » de la vie privée à sa « commercialisation ».

La vie privée s'est transformée et n'est plus une transaction où chaque individu serait seul face aux autres, mais une concertation où les motivations des citoyens se combinent pour créer des collectivités sociales (groupes de pression, association spécialisées, instances reconnaissables de porteurs d'intérêts) qui engagent une confrontation avec les organisations industrielles et les pouvoirs étatiques. La nature *éminemment collective de la négociation* qui se mène actuellement autour de la vie privée, permet de lire sa défense avant tout comme une confrontation conflictuelle et itérative visant à adapter les règles et les conditions d'usage des services aux besoins des utilisateurs. Ce processus est jalonné par une série de batailles et de controverses que les acteurs publics ont eu du mal à encadrer, dans un tâtonnement global impliquant société civile, propriétaires des grandes exploitations de données et organismes de renseignements étatiques.

Nul ne peut douter que cette négociation collective est indissociable de la protection des libertés individuelles, qui doivent être instrumentées sur le plan législatif afin de *contrebalancer les pouvoirs de négociation* entre ces différents acteurs. Le cadre législatif existant, encore basé sur une approche de *privacy as penetration* et sur l'effort de « laisser l'usager tranquille » en interrompant les flux de communication et les interconnexions, s'accorde mal avec les exigences centrales des citoyens d'une société en réseau, d'accéder à une maîtrise accrue sur leurs propres informations par l'éducation au numérique, par les initiatives de capacitation citoyenne, et par la mise en place d'infrastructures favorisant l'autonomie des communautés d'utilisateurs.

Immanquablement, cette vision ne s'accorde pas avec les orientations visant à mettre en place un régime de propriété privée sur les données personnelles – ce qui pourrait être qualifié de « privatisation de la *privacy* ». Le fait d'interpréter la *privacy* exclusivement comme un enjeu individuel, voir comme une entité monétisable et aliénable à merci, est parfois présenté comme une manière de compenser l'activité de monétisation des données personnelles que les grandes plateformes sociales du web et les intermédiaires de données (*data brokers*) réalisent déjà. C'est la position avancée par certains théoriciens du numérique tel Jaron Lanier qui, mettant en avant l'incapacité des libertés civiles à protéger la vie privée à l'heure d'Internet, prône le recours aux droits commerciaux *via*

l'institution d'un système de *micro-royalties*, que les entreprises du web devraient payer aux utilisateurs pour collecter, stocker et exploiter à des fins commerciales leurs données personnelles[183].

Provocation ou vision dystopique, des pas vers la réalisation de cette vision n'ont été jusqu'ici réalisés que par des start-up qui proposent des rémunérations pour les usagers de médias sociaux en échange de l'accès à leurs profils[184]. Déjà en 2011, le *World Economic Forum* décrivait les données personnelles comme des catégories d'actifs émergents (*emerging assets*)[185]. Cette désignation, qui en ferait l'un des « marchés répugnants » (tel celui des organes ou des droits de citoyenneté), pose un problème pour le législateur et pour les citoyens. Par ailleurs, dans un rapport de 2014, le Conseil national du numérique français s'est prononcé contre l'instauration d'un droit de propriété privée sur les données personnelles[186]. La principale raison invoquée, cohérente avec le besoin de respecter la nature collective de la négociation des données personnelles, a été d'équilibrer « *le rapport de force entre consommateurs et entreprises* » : la vente de donnée sous un régime de propriété privée ne pourrait générer que « *des revenus anecdotiques* », et déboucherait sur un renforcement des inégalités entre citoyens.

De surcroît, l'encadrement de ce débat, trop centré sur la dimension commerciale, gommerait le rôle des États en tant qu'acteurs de ce marché, en qualité d'acheteurs des données personnelles de citoyens à des fins de surveillance[187]. Dans un régime de propriété privée, les citoyens seraient d'autant moins en capacité de se défendre et leur pouvoir de négociation en serait alors affaibli.

Ces enjeux sont voués à devenir de plus en plus pressants dans un contexte d'élargissement de l'internet des objets. Ce dernier a comme conséquence immédiate un bouleversement de l'équilibre entre « l'Internet de publication » (qui comprend les contenus mis en ligne volontairement par les utilisateurs) et « l'Internet d'émission » (qui comprend les données et métadonnées émises par nos dispositifs connectés, avec peu ou point de possibilité de paramétrage ou de négociation de la part des citoyens). Dans ce nouvel aménagement le consentement au partage de ces données personnelles est en large mesure présupposé et non pas sollicité, ni jusque là accompagné par des démarches de sensibilisation et de prise de conscience des enjeux personnels et sociaux. La capture des données émises par compteurs, électroménagers et meubles « intelligents » placés dans

183. J. Lanier, *Who Owns the Future?*, New York : Simon & Schuster, 2013.

184. V. par exemple les efforts dans ce sens d'entreprises telles *YesProfile.com, Singly.com, Personal.com*, ou *Datacoup.com* qui proposent de « *récupérer la maîtrise et la propriété de vos données personnelles* ».

185. *World Economic Forum*, "Personal Data: The Emergence of a New Asset Class", 2013, consulté le 26 juin 2014, http://www.weforum.org/reports/personal-data-emergence-new-asset-class.

186. « Neutralité des plateformes : réunir les conditions d'un environnement numérique ouvert et soutenable », *Conseil National du Numérique,* consulté le 26 juin 2014, http://www.cnnumerique.fr/ plateformes/.

187. C. Soghoian, *The Spies We Trust : Third Party Service Providers and Law Enforcement Surveillance*, Indiana University, 2012.

les logements particuliers, ainsi que par les moyens de transport et par d'autres éléments ambiants des infrastructures urbaines (capteurs, caméras, etc.) est déjà une partie de notre réalité, mais est destinée à atteindre un seuil critique dans lequel ni les droits individuels, ni les mesures de protection de la propriété privée des informations personnelles pourraient suffire pour contrer les formes d'aliénation et de l'expropriation de plus en plus forte auxquelles les citoyens seraient exposés. Dans le contexte qui se prépare, une législation s'appuyant sur les droits individuels ne serait qu'un tigre de papier. Sortir du piège conceptuel de la « privatisation de la *privacy* » signifie autant reconnaître les dangers de la réduction marchande des éléments qui composent la vie connectée des citoyens, que la nécessité de sortir de la logique de la personnalisation de la vie privée, pour qu'elle devienne à plein titre un souci collectif, inscrit dans un cadre dans lequel les autonomies et les libertés soient respectées *by design*.

Liste des abréviations et des acronymes

AAI	Autorité administrative indépendante
AFNIC	Association française pour le nommage internet en coopération
AMF	Autorité des marchés financiers
ANSSI	Agence nationale de la sécurité des systèmes d'information
API	*Application Programming Interface*
ARCEP	Autorité de régulation des communications électroniques et des postes
CADA	Commission d'accès aux documents administratifs
CC	Conseil constitutionnel
CCass	Cour de cassation
CE	Conseil d'État
CEDH	Cour européenne des droits de l'homme
CGU	Conditions générales d'utilisation
CGSP	Commissariat général à la stratégie et à la prospective
CIL	Correspondant informatique et libertés
CJUE	Cour de justice de l'Union européenne
CNCIS	Commission nationale de contrôle des interceptions de sécurité
CNIL	Commission nationale de l'informatique et des libertés
CPCE	Code des postes et des communications électroniques
CSA	Conseil supérieur de l'audiovisuel
DARPA	*Defense Advanced Research Projects Agency*
DGSI	Direction générale de la sécurité Intérieure
DMP	Dossier médical personnel
DPSD	Direction nationale du renseignement et des enquêtes douanières
DRM	Direction du renseignement militaire
EDRi	*European Digital Rights* (réseau européen pour les droits numériques)
FAI	Fournisseur d'accès à internet
FAQ	*Frequently asked questions* (questions fréquemment posées)
FCC	*Federal Communications Commission*

FGI	Forum pour la gouvernance de l'internet
FNAED	Fichier national automatisé des empreintes digitales
FNAEG	Fichier national automatisé des empreintes génétiques
FFT	Fédération française des télécommunications
FPR	Fichier des personnes recherchées
FTC	*Federal Trade Commission*
GAC	*Governmental Advisory Committee*
GPS	*Global Positionning System* (système de localisation mondial)
HADOPI	Haute Autorité pour la diffusion des œuvres et la protection des droits sur Internet
HTTP	*Hypertext Transfer Protocol* (protocole de transfert hypertexte)
ICANN	*Internet Corporation for Assigned Names and Numbers* (Société pour l'attribution des noms de domaine et des numéros sur internet)
INRIA	Institut national de recherche en informatique et en automatique
JUDEX	Système judiciaire de documentation et d'exploitation
LCEN	Loi pour la confiance dans l'économie numérique
LICRA	Ligue internationale contre le racisme et l'antisémitisme
LOPSSI	Loi d'orientation et de programmation pour la performance de la sécurité intérieure
LPM	Loi de programmation militaire
MOOCs	*Massive Open Online Courses*
NIR	Numéro d'inscription au répertoire (de l'INSEE)
NSA	*National Security Agency* (Agence nationale de sécurité américaine)
OCLCTIC	Office central de lutte contre la criminalité liée aux technologies de l'information et de la communication
OIV	Opérateur d'importance vitale
OMPI	Organisation mondiale de la propriété intellectuelle
PNR	*Passenger Name Record*
RNIPP	Répertoire national d'identification des personnes physiques
SAFARI	Système automatisé pour les fichiers administratifs et le répertoire des individus
SMAD	Services de medias audiovisuels à la demande
SNIIRAM	Système national d'information interrégimes de l'assurance maladie
STAD	Systèmes de traitement automatisé des données
STIC	Système de traitement des infractions constatées
OACI	Organisation de l'aviation civile internationale
TAJ	Traitements d'antécédents judiciaires

TCP/IP	*Transmission Control Protocol / Internet Protocol* (protocole de contrôle de transmissions /protocole internet)
TFUE	Traité sur le fonctionnement de l'Union européenne
TRACFIN	Traitement du renseignement et d'action contre les services financiers clandestins
UIT	Union internationale des télécommunications
UPU	Union postale universelle
VTC	Véhicules de tourisme avec chauffeur
W3C	*World Wide Web Consortium*

Références bibliographiques

Rec.	Références consultables au Recueil Lebon
T.	Références consultables aux Tables du Recueil Lebon
<http://... >	Références consultables sur internet, les adresses mentionnées entre < > ayant été consultées entre janvier et juillet 2014
ArianeWeb	Références consultables dans la base de jurisprudence des décisions et avis contentieux du Conseil d'État et des cours administratives d'appel (décisions, analyses et avis ayant été retenus pour leur apport à la jurisprudence, sélection de conclusions de rapporteurs publics). <http://www.conseil-etat.fr/fr/base-de-jurisprudence/>

Table des matières

- **SOMMAIRE** 3
- **AVANT-PROPOS** 5
- **SYNTHÈSE** 9
- **INTRODUCTION** 35
- Première partie – **L'ESSOR DU NUMÉRIQUE A SUSCITÉ LA RECONNAISSANCE DE NOUVEAUX DROITS FONDAMENTAUX ET MODIFIÉ LEURS CONDITIONS D'EXERCICE** 41

1.1. L'essor du numérique entraîne des mutations techniques, économiques et sociales 42

– 1.1.1. Des révolutions techniques : la mise en réseau des machines, – la mise en données du monde 42
– 1.1.2. Des révolutions économiques : la valorisation par la donnée 53
– 1.1.3. Des révolutions de société : à nouvelles interactions, nouvelles normes – sociales ? 62

1.2. Le numérique a suscité la reconnaissance de nouveaux droits fondamentaux : le droit à la protection des données personnelles et le droit d'accès à internet 70

– 1.2.1. Le droit à la protection des données personnelles : un cadre juridique stable confronté à des enjeux radicalement nouveaux 70
– 1.2.2. Un nouveau droit fondamental de l'accès à internet 90

1.3. Le numérique a entraîné de profondes modifications du régime juridique de plusieurs libertés fondamentales 97

– 1.3.1. La liberté d'expression face au bouleversement des moyens de communication 98
– 1.3.2. De nouveaux espaces pour la liberté d'entreprendre, un encadrement juridique devenu plus complexe 104
– 1.3.3. Liberté personnelle : de nouvelles garanties face aux nouveaux instruments du droit à la sécurité 110
– 1.3.4. Le droit de la propriété intellectuelle confronté aux usages des réseaux 124

1.4. Internet n'échappe ni en fait, ni en droit à la puissance étatique, mais lui pose des défis inédits 132

– 1.4.1. La théorie selon laquelle internet échappe ou devrait échapper à la puissance de l'État apparaît aujourd'hui démentie 132
– 1.4.2. Internet soulève cependant des difficultés quant à son mode de gouvernance, à la détermination de la loi applicable et à l'effectivité des interventions de l'État 134

1.5. Le numérique, un espace de libertés et un enjeu stratégique 144

– 1.5.1 Le numérique ouvre de nouveaux espaces aux libertés 145
– 1.5.2. Le numérique est un enjeu stratégique, qui suscite une vive compétition entre États et entre acteurs économiques 147

■ Deuxième partie – **L'AMBIVALENCE DU NUMÉRIQUE NÉCESSITE DE REPENSER LA PROTECTION DES DROITS FONDAMENTAUX** 153

2.1. L'explosion des usages des données personnelles et des risques associés conduit à en repenser la protection 154

– 2.1.1. L'explosion des usages des données personnelles est porteuse d'une augmentation des risques pour les personnes concernées 154
– 2.1.2. Le cadre de la protection des données personnelles demeure pertinent
– dans ses principes.....165
– 2.1.3. Les instruments de la protection des données doivent en revanche être transformés.....175
– 2.1.4. L'arrêt *Google Spain* de la CJUE et la proposition de règlement européen relatif à la protection des données personnelles s'engagent à juste titre dans la voie de la réaffirmation des principes et de la rénovation des instruments ..184
– 2.1.5. La surveillance des communications par les pouvoirs publics présente des enjeux spécifiques et appelle des réponses adaptées.....194

2.2. Promouvoir les libertés à l'ère des « plateformes » 215

– 2.2.1. Neutralité des opérateurs de communications électroniques, loyauté des plateformes 217
– 2.2.2. Définir une répartition appropriée des rôles entre administration et plateformes dans la lutte contre les contenus illicites, dans le respect des prérogatives des juges.....225
– 2.2.3. La régulation des contenus licites, notamment des contenus audiovisuels,
– doit reposer sur des instruments adaptés à l'environnement numérique 231
– 2.2.4. Prendre la mesure du rôle joué par les algorithmes et concevoir l'encadrement de leur utilisation 233

2.3. Rendre applicables un socle de règles impératives pour tous les acteurs du numérique, quel que soit leur lieu d'établissement 240

– 2.3.1. Définir un socle de règles impératives applicables à tous les acteurs quel que soit leur lieu d'établissement.....240
– 2.3.2. Assurer une coopération efficace dans l'application, au sein de l'Union européenne et avec les autres systèmes juridiques 247
– 2.3.3. Remédier aux insuffisances du mode actuel de gouvernance d'internet 256

■ Troisième partie – **METTRE LE NUMÉRIQUE AU SERVICE DES DROITS INDIVIDUELS ET DE L'INTÉRÊT GÉNÉRAL** 261

3.1. Définir les principes fondant la protection des droits fondamentaux à l'ère du numérique..... 264

– 3.1.1. Le droit sur les données personnelles : un droit à l'autodétermination plutôt qu'un droit de propriété 264
– 3.1.2. Neutralité des réseaux, loyauté des plateformes.....270

3.2. Renforcer les pouvoirs des individus et de leurs groupements 274

– 3.2.1. Renforcer les capacités d'action individuelle 274
– 3.2.2. Renforcer les capacités d'action collective.....283

3.3. Redéfinir les instruments de la protection des droits fondamentaux et repenser le rôle des autorités publiques 289

– 3.3.1. Tirer les conséquences du passage à l'ère de l'économie des données personnelles 289
– 3.3.2. Définir un droit des algorithmes prédictifs 299
– 3.3.3. Organiser la répartition des rôles entre acteurs publics et acteurs privés dans la lutte contre les contenus illicites 304
– 3.3.4. Adapter les instruments de la promotion du pluralisme des médias 306
– 3.3.5. Développer la médiation pour régler les litiges liés à l'utilisation des technologies numériques 308

3.4. Assurer le respect des droits fondamentaux dans l'utilisation du numérique par les personnes publiques 309

– 3.4.1. Poursuivre l'ouverture des données publiques tout en prévenant les risques pour la vie privée 309
– 3.4.2. Renforcer les garanties entourant l'usage des fichiers de police judiciaire 314
– 3.4.3. Conjuguer le plein respect des droits fondamentaux et l'efficacité de la surveillance des communications électroniques à des fins de prévention des atteintes à la sécurité nationale 319

3.5. Organiser la coopération européenne et internationale 324

– 3.5.1. Affirmer l'applicabilité du droit européen et organiser la coopération au sein de l'Union européenne 324
– 3.5.2. Promouvoir de nouvelles formes de coopération avec les autres espaces juridiques 326
– 3.5.3. Rééquilibrer la gouvernance d'internet 329

■ **CONCLUSION** 333

■ **RÉCAPITULATIF DES MESURES PROPOSÉES** 337

■ **ANNEXES** 351

Annexe 1 – Liste des personnes auditionnées 353

Annexe 2 – « Groupe de contacts » de l'étude annuelle : constitution et composition 359

Annexe 3 – Numérique et santé 361

Annexe 4 – Numérique et éducation 373

Annexe 5 – Numérique et relations du travail 383

■ **CONTRIBUTIONS** 391

La jurisprudence américaine en matière de liberté d'expression sur Internet 393

Des données sans personne : le fétichisme de la donnée à caractère personnel à l'épreuve de l'idéologie des big data 407

Quatre thèses sur la surveillance numérique de masse et la négociation de la vie privée 423

■ **LISTE DES ABRÉVIATIONS ET DES ACRONYMES** 435

■ **TABLE DES MATIÈRES** 439